Innominate mGuard

Benutzerhandbuch

Software-Release 4.0.0

Innominate Security Technologies AG
Albert-Einstein-Str. 14
D-12489 Berlin
Tel.: +49 (0)800-366 4666
info@innominate.com
www.innominate.com

© Innominate Security Technologies AG

Juni 2006
„Innominate“ und „mGuard“ sind registrierte Handelsnamen der Innominate Security Technologies AG. Die mGuard Technologie ist durch die Patent 10138865 und 10305413, erteilt durch das Deutschen Patentamt, geschützt. Weitere Patente sind angemeldet.
Weder das Gesamtdokument noch Teile davon dürfen ohne schriftliche Genehmigung übertragen oder kopiert werden.
Die Innominate AG behält sich das Recht vor, jederzeit und ohne Benachrichtigung dieses Dokument zu verändern. Innominate übernimmt keine Gewährleistung für diese Unterlagen. Dies gilt ohne Einschränkung auch für die stillschweigende Zusicherung der Verkäuflichkeit und der Eignung für einen bestimmten Zweck.
Innominate übernimmt ferner keine Haftung für Fehler im vorliegenden Handbuch sowie für zufällige oder Folgeschäden im Zusammenhang mit der Lieferung, Leistung oder Verwendung dieser Unterlagen.
Ohne die vorherige schriftliche Zustimmung der Innominate Security Technologies AG darf dieses Handbuch weder teilweise noch vollständig fotokopiert, vervielfältigt oder in eine andere Sprache übersetzt werden.

Innominate Dokumentennummer: 574008-194

Inhalt

1 Einleitung ... 8
Netzwerk-Features ... 8
Firewall-Features ... 8
Anti-Virus-Features ... 8
VPN-Features ... 8
Weitere Features ... 9
Support ... 9
2 Typische Anwendungsszenarien ... 10
Stealthmodus ... 10
Netzwerkrouter ... 10
DMZ ... 10
VPN Gateway ... 11
WLAN über VPN ... 11
Internetzugang über VPN ... 12
Auflösen von Netzwerkkonflikten ... 13
3 Bedienelemente und Anzeigen ... 14
3.1 mGuard blade ... 14
3.2 mGuard delta ... 15
3.3 mGuard industrial ... 16
3.4 mGuard smart ... 17
3.5 mGuard PCI ... 18
4 Inbetriebnahme ... 19
4.1 Lieferumfang ... 20
4.2 mGuard blade anschließen ... 21
Inbetriebnahme mGuard bladeBase ... 21
Kontrolleinheit (CTRL Slot) ... 21
Anschluss mGuard blade ... 22
4.3 mGuard industrial anschließen ... 23
4.4 mGuard delta anschließen ... 24
Klemmblock ... 24
Erdungsanschluss ... 24
Inbetriebnahme ... 25
Netzwerkverbindung ... 25
Demontage ... 25
4.5 mGuard PCI anschließen ... 27
4.5.1 Auswahl Treibermodus oder Power-over-PCI Modus ... 27
Treibermodus ... 27
Power-over-PCI Modus ... 28
4.5.2 Einbau der Hardware ... 30
4.5.3 Treiber Installation ... 31
Windows XP ... 31
Windows 2000 ... 32
Linux ... 34
4.6 mGuard smart anschließen ... 36
5 Konfiguration vorbereiten ... 37
5.1 Anschließen des mGuards ... 37
mGuard blade ... 37
mGuard delta ... 37
mGuard industrial ... 37
mGuard smart ... 37
mGuard PCI ... 37
5.2 Lokale Konfiguration: Bei Inbetriebnahme ... 38

5.2.1 mGuard blade, industrial und smart ... 38
Bei konfigurierter Netzwerk-Schnittstelle ... 38
Bei nicht konfigurierter Netzwerk-Schnittstelle ... 38
5.2.2 mGuard delta ... 39
5.2.3 mGuard PCI ... 40
Installieren der mGuard Karte ... 40
Installieren der mGuard Treiber ... 40
Konfiguration der Netzwerk-Schnittstelle ... 40
Standardgateway ... 41
5.3 Lokale Konfigurationsverbindung herstellen ... 42
Web-basierte Administratoroberfläche ... 42
Bei erfolgreichem Verbindungsaufbau ... 43
5.4 Fernkonfiguration ... 44
Voraussetzung ... 44
Fernkonfiguration ... 44
6 Konfiguration ... 45
6.1 Bedienung ... 45
6.2 Menü Verwaltung ... 48
6.2.1 Verwaltung → Systemeinstellungen ... 48
Host ... 48
Meldekontakt (nur industrial) ... 50
Zeit und Datum ... 51
Shell Zugang ... 52
6.2.2 Verwaltung →Web Einstellungen ... 54
Grundeinstellungen ... 54
Zugriff ... 54
6.2.3 Verwaltung →Lizensierung ... 56
Übersicht ... 56
Installieren ... 57
6.2.4 Verwaltung →Update ... 58
Übersicht ... 58
Update ... 59
Anti-Virus Muster ... 60
6.2.5 Verwaltung →Konfigurationsprofile ... 61
Backup / Restore ... 61
Profile auf dem ACA11 (nur industrial) ... 62
6.2.6 Verwaltung →SNMP (nur enterprise) ... 63
Abfrage ... 63
Trap ... 65
LLDP ... 68
6.2.7 Verwaltung →Zentrale Verwaltung ... 69
Konfiguration holen ... 69
6.2.8 Verwaltung →Redundanz (nur enterprise XL) ... 70
Redundanz ... 71
ICMP Checks ... 72
6.2.9 Verwaltung →Neustart ... 73
Restart ... 73
6.3 Menü Bladekontrolle (nur blade Controller) ... 74
6.3.1 Bladekontrolle → Übersicht ... 74
6.3.2 Bladekontrolle → Blade 01 bis 12 ... 75
Blade in slot #__ ... 75
Konfiguration ... 75
6.4 Menü Netzwerk ... 77

6.4.1 Netzwerk →Interfaces 77
Allgemein 77
Netzwerk Modus → Stealth (Werkseinstellung außer mGuard delta) 79
Netzwerk Modus → Router (Werkseinstellung mGuard delta) 81
Netzwerk Modus → PPPoE 83
Netzwerk Modus → PPTP 84
Netzwerk Modus → Router, PPPoE oder PPTP 85
Ethernet 86
Serielle Schnittstelle 87
Hardware 89
6.4.2 Netzwerk →DNS 89
DNS Server 89
DynDNS 90
6.4.3 Netzwerk →DHCP 91
..... 91
6.5 Menü Benutzerauthentifizierung 95
6.5.1 Benutzerauthentifizierung →Lokale Benutzer 95
Passwords 95
6.5.2 Benutzerauthentifizierung →Externe Benutzer 96
Remote Users 96
Radius Server 97
Status 97
6.6 Menü Netzwerksicherheit (nicht blade Controller) 98
6.6.1 Netzwerksicherheit → Packet Filter 98
Eingangsregeln 98
Ausgangsregeln 99
MAC Filter 100
Erweiterte Einstellungen 101
6.6.2 Netzwerksicherheit → NAT 103
Masquerading 103
DNAT 104
Connection Tracking 106
6.6.3 Netzwerksicherheit → DoS-Schutz 107
Flood Protection 107
6.6.4 Netzwerksicherheit → Benutzerfirewall 108
Benutzerfirewall-Templates 108
6.6.5 Benutzerfirewall → Template definieren 109
Allgemein 109
Template Nutzer 109
Firewall Regeln 109
6.7 Menü Web-Sicherheit (nicht blade Controller) 111
6.7.1 Web-Sicherheit →HTTP 111
Virenschutz 111
..... 111
6.7.2 Web-Sicherheit →FTP 113
Virenschutz 113
6.8 Menü E-Mail-Sicherheit (nicht blade Controller) 116
6.8.1 E-Mail-Sicherheit →POP3 116
Virenschutz 116
6.8.2 E-Mail-Sicherheit →SMTP 119
Virenschutz 119
6.9 Menü IPsec VPN (nicht blade Controller) 122
6.9.1 IPsec VPN → Global 122
Maschinen Zertifikat 122

DynDNS-Überwachung ... 123
6.9.2 IPsec VPN → Verbindungen ... 124
Verbindungen ... 124
6.9.3 VPN-Verbindung definieren ... 125
Allgemein: ... 125
Authentifizierung ... 128
Firewall ... 130
IKE Optionen ... 132
6.9.4 IPsec VPN → L2TP über IPsec ... 134
L2TP Server ... 134
6.9.5 IPsec VPN → IPsec Status ... 135
6.10 Menü Logging ... 136
6.10.1 Logging → Einstellungen ... 136
Remote Logging ... 136
6.10.2 Logging → Logs ansehen ... 137
Netzwerksicherheit ... 137
AntiVirus ... 137
AntiVirus Update ... 138
IPsec VPN ... 138
6.11 Menü Support ... 139
6.11.1 Support → Erweitert ... 139
Hardware ... 139
Snapshot ... 139
6.12 CIDR (Classless InterDomain Routing) ... 140
6.13 Netzwerk-Beispielskizze ... 141
7 Die Rescue-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware ... 142
7.1 Neustart durchführen ... 142
7.2 Recovery-Prozedur ausführen ... 142
7.3 Flashen der Firmware ... 143
Voraussetzungen zum Flashen der Firmware: DHCP- und TFTP-Server ... 145
DHCP- und TFTP-Server unter Windows installieren ... 145
DHCP- und TFTP-Server unter Linux installieren ... 146
8 Glossar ... 147
Asymmetrische Verschlüsselung ... 147
DES / 3DES ... 147
AES ... 147
Client / Server ... 147
Datagramm ... 148
Default Route ... 148
DynDNS-Anbieter ... 148
IP-Adresse ... 149
IPsec ... 150
NAT (Network Address Translation) ... 150
Port-Nummer ... 151
Proxy ... 151
PPPoE ... 151
PPTP ... 151
Router ... 151
Trap ... 151
X.509 Zertifikat ... 151
Protokoll, Übertragungsprotokoll ... 152
Service Provider ... 152
Spoofing, Antispoofing ... 152
Symmetrische Verschlüsselung ... 152

TCP/IP (Transmission Control Protocol/Internet Protocol) 153
VLAN 153
VPN (Virtuelles Privates Netzwerk) 153
9 Technische Daten 154
Allgemein 154
mGuard industrial 154

1 Einleitung

Der mGuard sichert IP-Datenverbindungen. Dazu vereinigt das Gerät folgende Funktionen:

- Netzwerk Karte (mGuard PCI), Switch (mGuard delta)
- VPN-Router (VPN - Virtuelles Privates Netzwerk) für sichere Datenübertragung über öffentliche Netze (hardwarebasierte DES, 3DES und AES Verschlüsselung, IPsec Protokoll)
- Konfigurierbare Firewall für den Schutz vor unberechtigtem Zugriff. Der dynamische Paketfilter untersucht Datenpakete anhand der Ursprungs- und Zieladresse und blockiert unerwünschten Datenverkehr.
- Virenschutz mit Unterstützung für die Protokolle HTTP, FTP, SMTP und POP3

Die Konfiguration des Gerätes erfolgt einfach mit einem Web-Browser.

Netzwerk-Features

- Stealth (Auto, Static, Multi), Router (Static, DHCP Client), PPPoE (für DSL) und PPTP (für DSL)
- VLAN
- DHCP Server/Relay auf den internen und externen Netzwerkschnittstellen
- DNS Cache auf den internen Netzwerkschnittstelle
- Administration über HTTPS und SSH

Firewall-Features

- Stateful Packet Inspection
- Anti-Spoofing
- IP Filter
- L2 Filter (nur im Stealth Mode)
- NAT mit FTP, IRC und PPTP Unterstützung (nur in den Router Modi)
- 1:1 NAT (nur in den Router Modi)
- Port Forwarding (nur in den Router Modi)
- Firewalldurchsatz maximal 99MBit/s
- Individuelle Firewallregeln für verschiedene Nutzer (Benutzerfirewall)

Anti-Virus-Features

- ClamAV-Virenschutz
- Unterstützte Protokolle: HTTP, FTP, POP3 und SMTP (senden)
- Der Virenfilter kann die folgenden Formate dekomprimieren:
    - ZIP
    - RAR
    - GZIP
    - BZIP2
    - TAR
    - MS OLE2
    - MS Cabinet Dateien (CAB)
    - MS CHM (Komprimiertes HTML)
    - MS SZDD
    - UPX
    - FSG
    - Petite

VPN-Features

- Protokoll: IPsec (Tunnel und Transport Mode)
- IPsec DES Verschlüsselung mit 56 Bit
- IPsec 3DES Verschlüsselung mit 168 Bit
- IPsec AES Verschlüsselung mit 128, 192 und 256 Bit
- Paket-Authentifizierung: MD5, SHA-1
- Internet Key Exchange (IKE) mit Main und Quick Mode
- Authentisierung: Pre-Shared Key (PSK), X.509v3 Zertifikate
- DynDNS
- NAT-T

- Dead Peer Detection (DPD)
- Hardwareverschlüsselung
- bis zu 250 VPN Tunnel
- VPN Durchsatz max. 35MBit/s bei 266MHz und 70MBit/s bei 533MHz
- IPsec/L2TP Server
- IPsec Firewall und 1:1 NAT
- Defaultroute über VPN

Weitere Features

- MAU Management
- Remote Logging
- Router/Firewall Redundanz
- LLDP
- Administration using SNMP v1-v3 und Innominate Security Configuration Manager (ISCM)

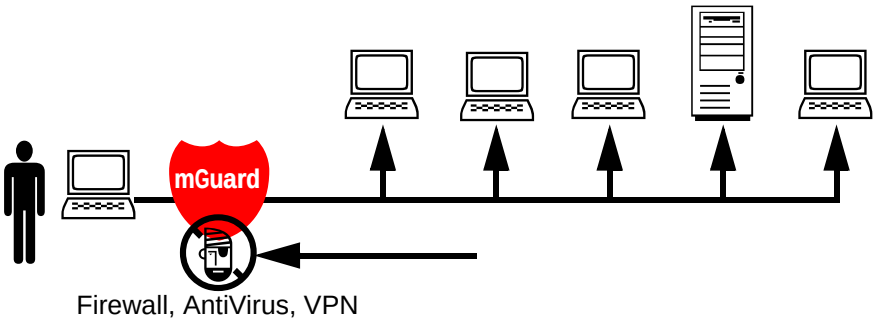
Support

Bei Problemen mit Ihrem mGuard wenden Sie sich bitte an Ihren Händler. Zusätzliche Informationen zum Gerät, sowie Release Notes und Software-Updates finden Sie unter folgender Internet-Adresse: http://www.innominate.de/

2 Typische Anwendungsszenarien

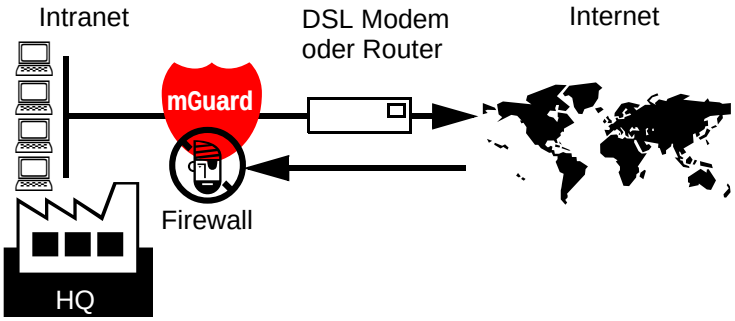
Nachfolgend werden verschiedene mögliche Anwendungsszenarien für den mGuard skizziert.

Stealthmodus



Im *Stealth* Modus (Werkseinstellung) kann der mGuard zwischen einen einzelnen Rechner und das übrige Netzwerk gesetzt werden.
Die Einstellungen für Firewall, AntiVirus und VPN können mit einem Webbrowser unter der URL https://1.1.1.1/ vorgenommen werden.
Auf dem Rechner selbst müssen keine Konfigurationsänderungen durchgeführt werden.

Netzwerkrouter

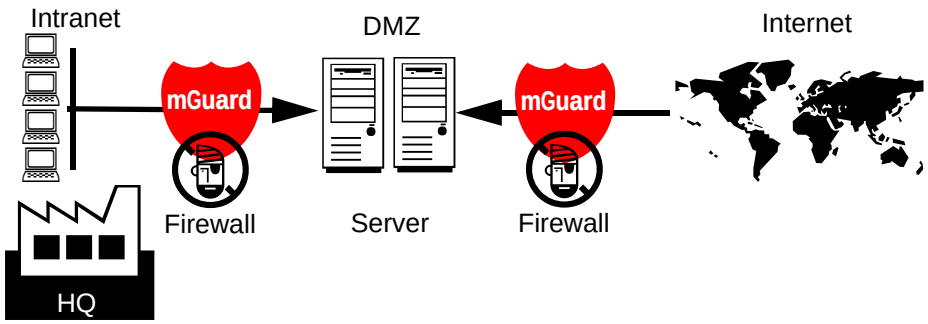


Der mGuard kann für mehrere Rechner als Netzwerkrouter die Internetanbindung bereitstellen und das Firmennetz dabei mit seiner Firewall schützen.
Dazu kann einer der folgenden Netzwerk-Modi des mGuard genutzt werden:

- *Router*, wenn der Internet-Anschluss z.B. über einen DSL-Router oder eine Standleitung erfolgt.
- *PPPoE*, wenn der Internet-Anschluss z.B. per DSL-Modem erfolgt und das PPPoE-Protokoll verwendet wird (z.B. in Deutschland).
- *PPTP*, wenn der Internet-Anschluss z. B. per DSL-Modem erfolgt und das PPTP-Protokoll verwendet wird (z. B. in Österreich).

Bei Rechnern im Intranet muss der mGuard als Defaultgateway festgelegt sein.

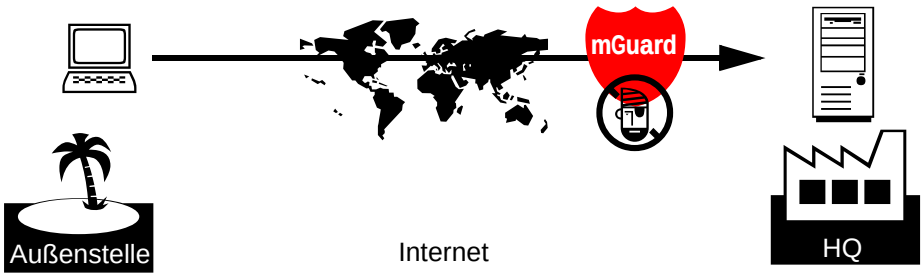
DMZ



Eine DMZ (Demilitarized Zone, deutsch: entmilitarisierte Zone) ist ein geschütztes Netzwerk, das zwischen zwei anderen Netzen liegt. Z.B. kann sich die Webpräsenz einer Firma so in der DMZ befinden, dass nur aus dem Intranet heraus mittels FTP neue Seiten auf den Server kopiert werden können, der lesende

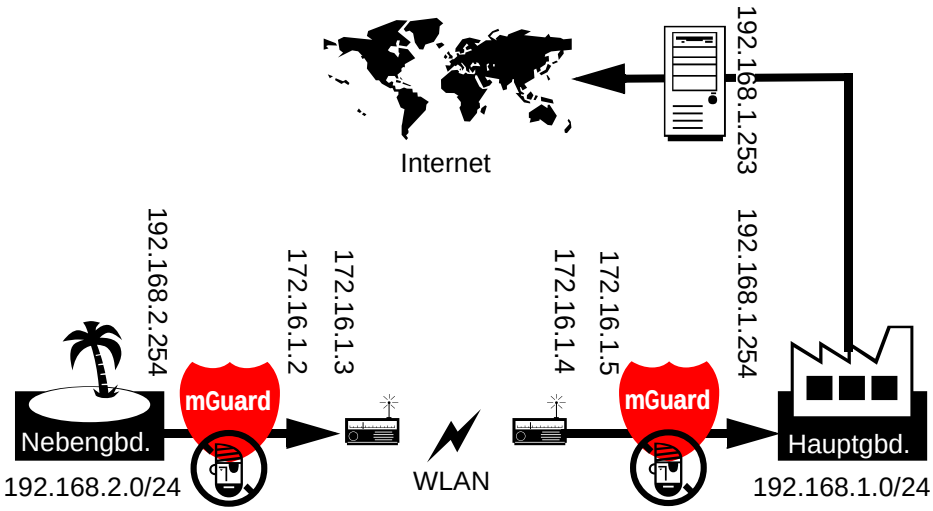
Zugriff per HTTP auf die Seiten jedoch auch aus dem Internet heraus möglich ist. Die IP Adressen innerhalb der DMZ können öffentlich sein, oder aber privat, wobei der mit dem Internet verbundene mGuard die Verbindungen mittels Port-forwarding an die privaten Adressen innerhalb der DMZ weiterleitet.

VPN Gateway



Mitarbeitern einer Firma soll ein verschlüsselter Zugang zum Firmennetz von zu Hause oder von unterwegs aus zur Verfügung gestellt werden. Der mGuard übernimmt dabei die Rolle des VPN Gateways.
Auf den externen Rechnern muss dazu eine IPsec fähige VPN-Client Software installiert werden. Oder das Betriebssystem muss diese Funktionalität bereits unterstützen, wie z.B. Windows 2000/XP.

WLAN über VPN



Zwei Gebäude einer Firma sollen über eine mit IPsec geschützte WLAN Strecke miteinanderverbunden werden. Vom Nebengebäude soll zudem der Internetzugang des Hauptgebäudes mitgenutzt werden können.

In diesem Beispiel wurden die mGuards in den *Router-M*odus geschaltet und für das WLAN ein eigenes Netz mit 172.16.1.x Adressen eingerichtet.
Da vom Nebengebäude aus das Internet über das VPN erreichbar sein soll, wird hier eine aktive Default Route über das VPN eingerichtet:

Verbindungstyp	Tunnel (Netz <-> Netz)
Adresse des lokalen Netzes	192.168.2.0/24
Adresse des gegenüberliegenden Netzes	0.0.0.0/0

Im Hauptgebäude wird das entsprechende Gegenstück der Verbindung konfiguriert:

Verbindungstyp	Tunnel (Netz <-> Netz)

Die dazugehörige Netzmaske	0.0.0.0
Adresse des gegenüberliegenden Netzes	192.168.2.0/24

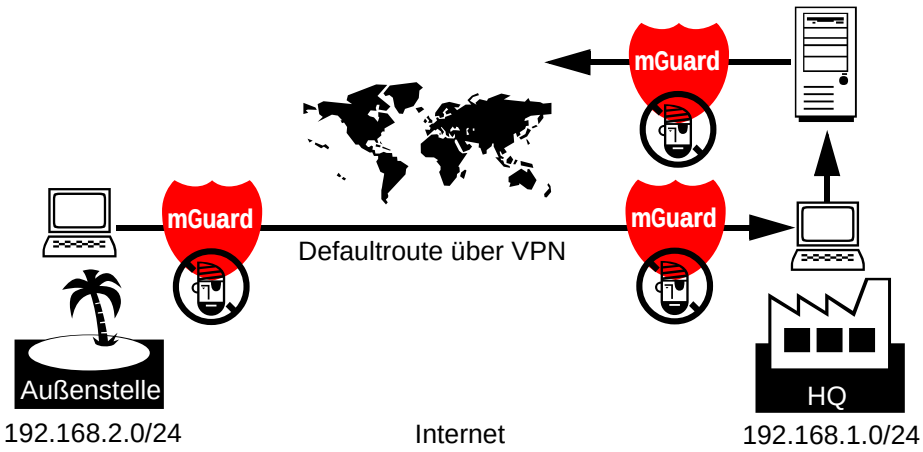
Die Default Route eines mGuards führt normalerweise immer über das externe Interface. In diesem Fall führt der Weg ins Internet und somit auch die Default Route, über die IP 192.168.1.253. Dazu muss beim mGuard im Hauptgebäude unter „Netzwerk →Interfaces", „Allgemein"eine aktive Default Route definiert werden

Zusätzliche interne Routen	Netzwerk	Gateway
	0.0.0.0/0	192.168.1.253

und eine externe Route auf die IPs 172.168.1.2 und 172.168.1.3 eingerichtet werden

Zusätzliche externe Routen	Netzwerk	Gateway
	172.16.1.2/1	172.16.1.4

Internetzugang über VPN



Im oberen Szenario soll der Internetzugang der Außenstellen einer Firma über einen zentralen Server erfolgen, welcher den Zugang auf bestimmte Webseiten blockiert, Viren filtert, etc..
Dafür muss in der Außenstelle (links) mit dem lokalen Netz 192.168.2.0/24 eine aktive Defaultroute über das VPN angelegt werden[1]:

Verbindungstyp	Tunnel (Netz <-> Netz)
Lokales Netzwerk	192.168.2.0/24
Gegenüberliegendes Netzwerk	0.0.0.0/0

1. Diese Defaultroute gilt nur für vom mGuard weitergeleiteten Datenverkehr, nicht aber für die VPN Verbindung als solche oder DNS, NTP und ähnliche Verbindungen, die der mGuard von sich aus initiiert.

Der VPN Tunnel der Gegenstelle wird entsprechend konfiguriert:

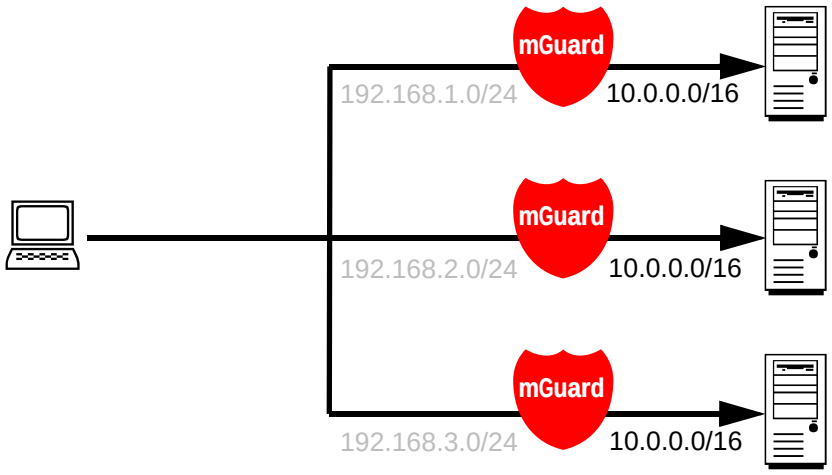
Verbindungstyp	Tunnel (Netz <-> Netz)
Lokales Netzwerk	0.0.0.0/0
Gegenüberliegendes Netzwerk	192.168.2.0/24

Da VPN Verbindungen nur über das externe Interface (WAN) aufgebaut werden, muß die Route zum Internet auf der Gegenstelle über das lokale Interface (LAN) eingerichtet werden. Dazu muß unter “Netzwerk > Interfaces”, “Interne Netzwerke”, “Zusätzliche interne Routen” eine lokalte Defaultroute konfiguriert werden:

Netzwerk	Gateway
0.0.0.0/0	192.168.2.254

(Wobei 192.168.2.254 hier das Internetgateway in dem Netzwerk auf der rechten Seite der obigen Zeichnung sei.)

Auflösen von Netzwerkkonflikten

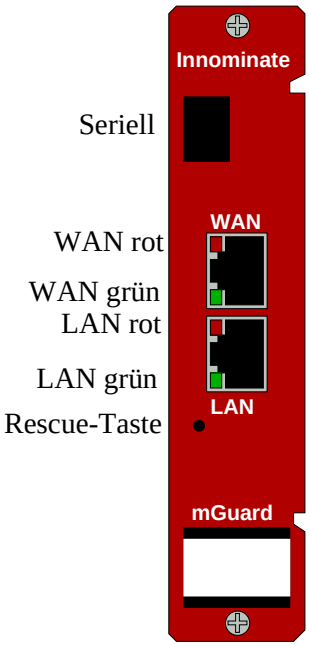


In der obigen Zeichnung sollen die Netzwerke auf der rechten Seite von dem Netzwerk oder Rechner auf der linken Seite erreichbar sein. Aus historischen oder technischen Gründen überschneiden sich jedoch die Netzwerke der Rechner auf der rechten Seite.
Mit Hilfe der mGuards und ihrem 1:1 NAT Feature können diese Netze nun auf andere Netze umgeschrieben werden, so dass der Konflikt aufgelöst wird.

(1:1 NAT kann im normalen Routing und in IPsec VPN Tunnel genutzt werden.)

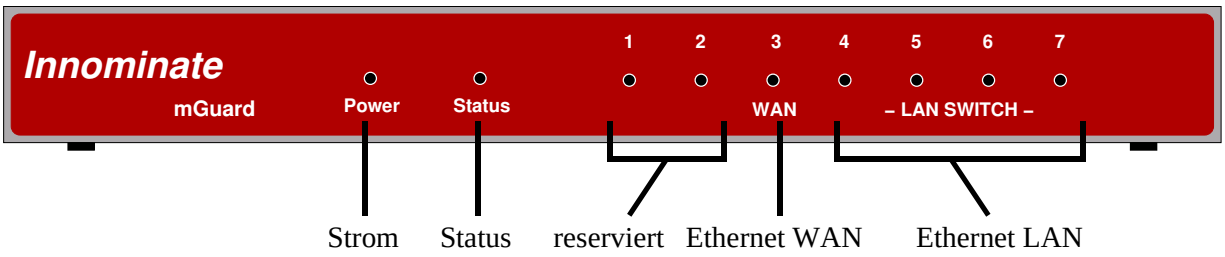
3 Bedienelemente und Anzeigen

3.1 mGuard blade



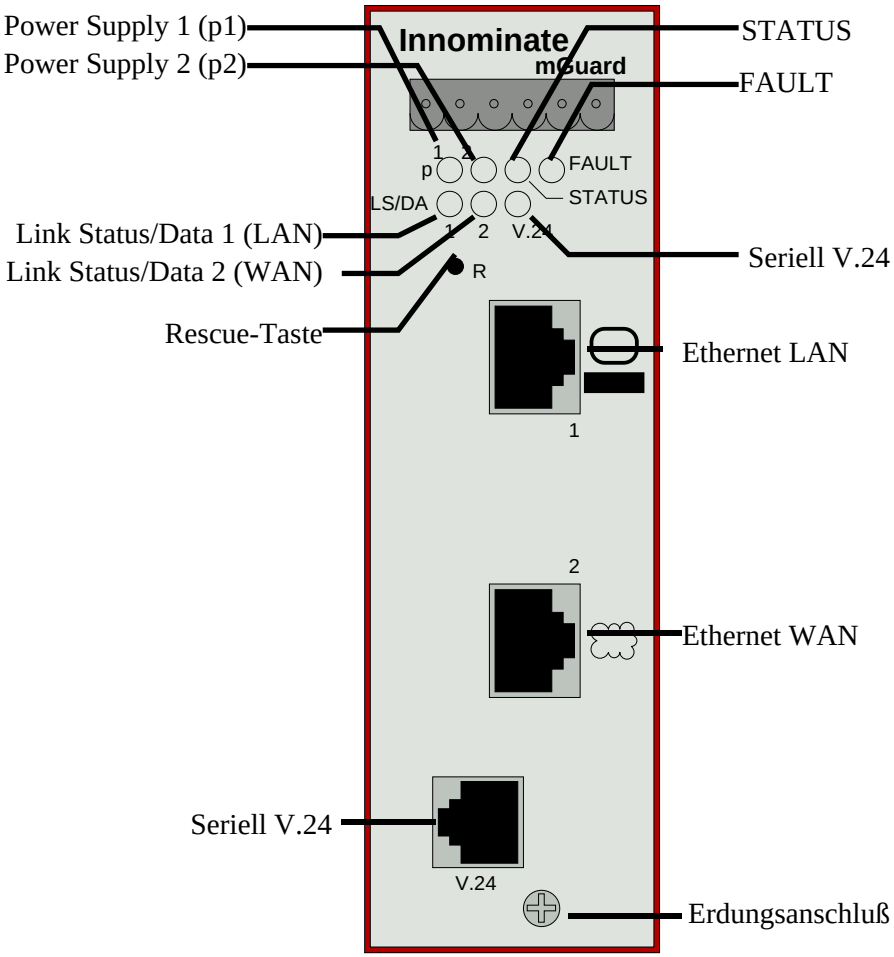
LEDs	Zustand	Bedeutung
WAN Rot, LAN Rot	blinkend	**Bootvorgang**. Nach dem Starten oder Neustarten des Rechners.
WAN Rot	blinkend	**Systemfehler**. ⌦ Führen Sie einen Neustart durch. Dazu die **Rescue**-Taste kurz (1,5 Sek.) drücken Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen” auf Seite 142) oder wenden Sie sich an den Support.
WAN Grün, LAN Grün	leuchtend oder blinkend	**Ethernetstatus**. Zeigt den Status vom LAN bzw. WAN Interface. Sobald das Gerät angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner besteht. Bei der Übertragung von Datenpaketen erlischt kurzzeitig die LED.
WAN Grün, WAN Rot, LAN Grün	div. LED-Leuchtcodes	**Recovery-Modus**. Nach Drücken der **Rescue**-Taste. Siehe „Die Rescue-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware” auf Seite 142

3.2 mGuard delta



LEDs	State	Meaning
Power	ein	Die Stromversorgung ist aktiv.
Status	ein	Der mGuard startet.
	Herzschlag (aufleuchten, aufleuchten, Pause, ...)	Der mGuard ist bereit.
1,2	-	Reserviert
3 (WAN)	ein	Link vorhanden
	blinkend	Datentransfer
4-7 (LAN)	ein	Link vorhanden
	blinkend	Datentransfer

3.3 mGuard industrial

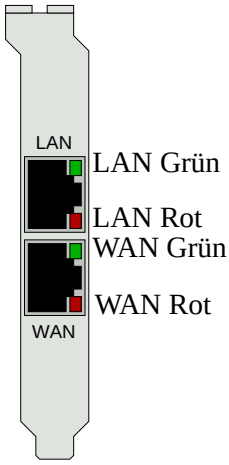


LEDs	Zustand	Bedeutung
p1, p2	grün leuchtend	Die Stromversorgung 1 bzw. 2 ist aktiv.
STATUS	grün blinkend	Der mGuard bootet.
	grün leuchtend	Der mGuard ist bereit.
	gelb leuchtend	Der mGuard ist bereit und Redundancy Master.
	gelb/grün blinkend	Der mGuard ist bereit und Redundancy Slave.
FAULT	rot	Der Meldekontakt ist in Folge eines Fehlers offen.
LS/DA 1/2 V.24	grün	Link vorhanden
	gelb blinkend	Datentransfer

3.4 mGuard smart

LEDs	Farbe	Zustand	Bedeutung
2	Rot/Grün	rot-grün blinkend	**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
	Grün	blinkend	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
	Rot	blinkend	**Systemfehler**. ⌧ Führen Sie einen Neustart durch. Dazu die Recovery-Taste kurz (1,5 Sek.) drücken ODER Das Gerät von der Stromversorgung kurz trennen und dann wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen” auf Seite 142) oder wenden Sie sich an den Support.
1 und **3**	Grün	leuchtend oder blinkend	**Ethernetstatus**. LED 1 zeigt den Status des internen Interface, LED 3 den Status des externen. Sobald das Gerät am Netzwerk angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner besteht. Bei der Übertragung von Datenpaketen erlischt kurzzeitig die LED.
1, 2, 3	div. LED-Leuchtcodes		**Recovery-Modus**. Nach Drücken der **Recovery**-Taste. Siehe „Die Rescue-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware” auf Seite 142.

3.5 mGuard PCI



LEDs	Zustand	Bedeutung
WAN Rot, LAN Rot	blinkend	**Bootvorgang**. Nach dem Starten oder Neustarten des Rechners.
WAN Rot	blinkend	**Systemfehler**. ⌧ Führen Sie einen Neustart durch. Dazu die **Rescue**-Taste kurz (1,5 Sek.) drücken ODER Starten Sie den Computer neu. Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen” auf Seite 142) oder wenden Sie sich an den Support.
WAN Grün, LAN Grün	leuchtend oder blinkend	**Ethernetstatus**. Zeigt den Status vom LAN bzw. WAN Interface. Sobald das Gerät angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner besteht. Bei der Übertragung von Datenpaketen erlischt kurzzeitig die LED.
WAN Grün, WAN Rot, LAN Grün	div. LED-Leuchtcodes	**Recovery-Modus**. Nach Drücken der **Rescue**-Taste. Siehe „Die Rescue-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware” auf Seite 142

4 Inbetriebnahme

Sicherheits-hinweise

Der Innominate mGuard ist für den Betrieb bei Schutzkleinspannung vorgesehen. Schließen Sie die Netzwerkinterfaces des mGuard nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen. Der mGuard darf nicht an Fernmeldeanschlüssen betrieben werden.

Warnung mGuard PCI! Berühren Sie vor Einbau des mGuard PCI den freien Metallrahmen ihres PCs, um Ihren Körper elektrostatisch zu entladen.

Warnung! Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Massnahmen durchzuführen.

Allgemeine Hinweise zur Benutzung

- mGuard PCI: Ihr PC muß einen freien PCI Slot (3,3V oder 5V) bereitstellen.
- Zum Reinigen des Gerätegehäuses ein weiches Tuch verwenden. Kein aggressives Lösungsmittel auftragen!
- Umgebungsbedingungen:
  0 bis +40°C (smart, blade) 55°C (PCI) 60°C (industrial)
- max. Luftfeuchtigkeit 90% (industrial: 95%), nicht kondensierend
- Nicht direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aussetzen, um Überhitzung zu vermeiden.
- Anschlusskabel nicht knicken. Den Netzwerkstecker nur zum Verbinden mit einem Netzwerk benutzen.

Schritte zur Inbetriebnahme

Um das Gerät in Betrieb zu nehmen, führen Sie folgende Schritte in der angegebenen Reihenfolge aus:

Schritt	Ziel	Seite
1	Lieferumfang prüfen, Release Notes lesen	„Lieferumfang” auf Seite 20
2	Gerät anschließen	• „mGuard blade anschließen” auf Seite 21 • „mGuard industrial anschließen” auf Seite 23 • „mGuard PCI anschließen” auf Seite 27 • „mGuard smart anschließen” auf Seite 36
3	Das Gerät konfigurieren, soweit erforderlich. Gehen Sie dazu die einzelnen Menüoptionen durch, die Ihnen der mGuard mit seiner Konfigurationsoberfläche bietet. Lesen Sie deren Erläuterungen in diesem Handbuch, um zu entscheiden, welche Einstellungen für Ihre Betriebsumgebung erforderlich oder gewünscht sind.	„Lokale Konfiguration: Bei Inbetriebnahme” auf Seite 38

4.1 Lieferumfang

Prüfen Sie vor Inbetriebnahme die Lieferung auf Vollständigkeit:

Zum Lieferumfang gehören

- Das Gerät *mGuard blade, delta, industrial, PCI oder smart*
- Handbuch im Portable Document Format (PDF) auf CD
- Quick Installation Guide

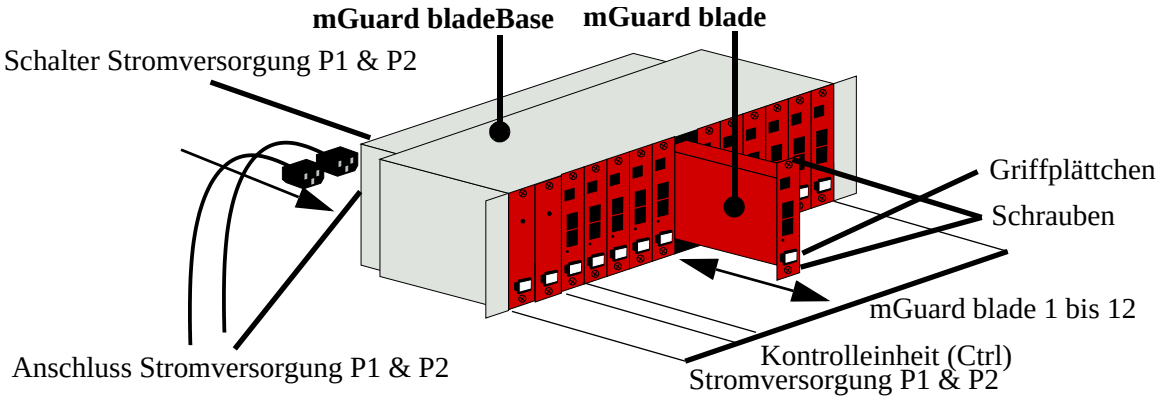
Das mGuard bladePack enthält weiterhin:

- Die 19’’ mGuard bladeBase
- 1 mGuard blade als Controller
- 2 Netzteile
- 2 Netzkabel
- 12 Leerblenden
- 12 Beschriftungsplätchen M1 bis M12
- Schrauben zur Montage der bladeBase

Der mGuard delta enthält weiterhin:

- eine 5V DC Stromversorgung
- zwei UTP Ethernetkabel
- ein serielles RS232 Kabel

4.2 mGuard blade anschließen



Inbetriebnahme mGuard bladeBase

- Bauen Sie den mGuard bladeBase in das Rack ein, z.B. in der Nähe des Patchfeldes.
- Versehen Sie die beiden Stromversorgungen und die Kontrolleinheit an der Vorderseite von links nach rechts mit den Griffplättchen „P1“, „P2“ und „Ctrl“.
- Verbinden Sie die beiden Stromversorgungen auf der Rückseite des mGuard bladeBase mit 100V oder 220/240V.
- Schalten Sie die beiden Stromversorgungen ein.
- Die LEDs an der Vorderseite der Stromversorgungen leuchten nun grün.

⌦ **Unbedingt darauf achten, dass eine ausreichende Luftzirkulation für das BladePack sichergestellt ist!**

⌦ **Bei Stapelung von mehreren BladePacks müssen 1 oder mehrere Zoll Lüftereinschübe vorgesehen werden, damit die aufgestaute Warmluft abgeführt werden kann!**

- Lösen Sie an der Blende bzw. an das zu ersetzende mGuard blade die obere und untere Schraube.
- Nehmen Sie die Blende ab bzw. ziehen Sie das alte mGuard blade heraus.
- Setzen Sie das neue mGuard blade mit der Leiterplatte in die Kunststofffüh-rungen und schieben Sie es vollständig in das mGuard bladeBase hinein.
- Sichern Sie das mGuard blade durch leichtes Anziehen der Schrauben.
- Ersetzen Sie das leere Griffplätchen durch das mit der passenden Nummer aus dem Zubehör der mGuard bladeBase. Oder ersetzen Sie es durch das des ausgetauschten mGuard blade. Dazu das Plättchen seitlich hinein- bzw. her-ausschieben.

⌦ Die mGuard bladeBase braucht beim Ein- und Ausbau eines mGuard blade nicht ausgeschaltet zu werden.

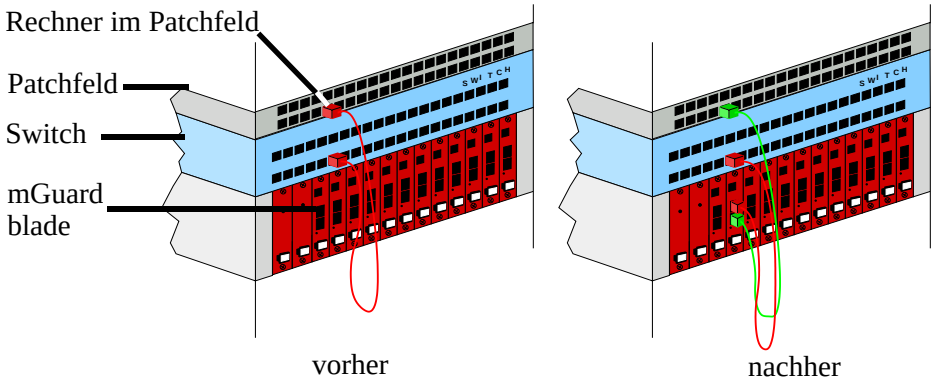
Kontrolleinheit (CTRL Slot)

Direkt neben den beiden Stromversorgungen befindet sich der „CTRL“ Slot. Ein darin betriebener mGuard blade arbeitet als Controller für alle anderen mGuard blades.

Bei der ersten Installation eines mGuard blade in den „CTRL“ Slot konfiguriert sich das blade in eine Kontrolleinheit wie folgt um:

- Die Benutzeroberfläche wird für den Betrieb als Controller umkonfiguriert.
- Er schaltet sich in den Router-Modus mit der lokalen IP 192.168.1.1.
- Die Funktionen Firewall, Anti-Virus und VPN werden zurückgesetzt und deaktiviert.

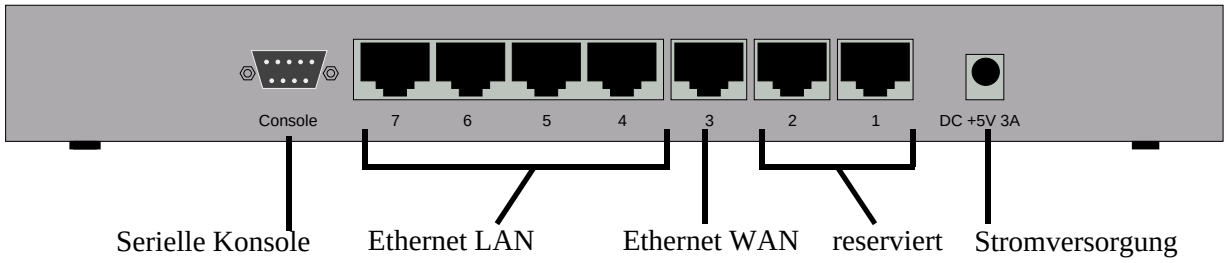
Anschluss mGuard blade



Wenn Ihr Rechner bereits an einem Netzwerk angeschlossen ist, dann patchen Sie das mGuard blade zwischen die bereits bestehende Netzwerkverbindung. Beachten Sie bitte, dass die Konfiguration zunächst nur über das LAN Interface erfolgen kann und die Firewall des mGuard allen IP Datenverkehr vom WAN zum LAN Interface unterbindet.

- Es ist keine Treiber-Installation erforderlich.
- Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern.

4.3 mGuard industrial anschließen

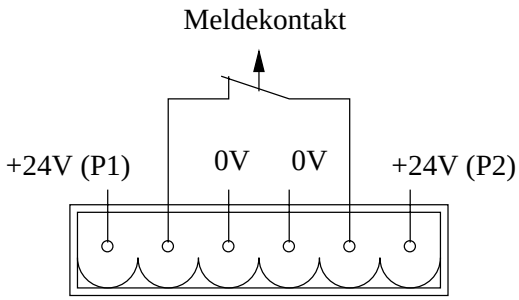


- Verbinden Sie die Stromversorgung (5V DC, 3A) mit der Buchse “DC +5V, 3A” des mGuards.
- Verbinden Sie Ihren lokalen Computer oder lokales Netzwerk mittels eines UTP Ethernetkabels (CAT 5) mit einem der Ethernet LAN Anschlüße (4 bis 7) des mGuards.

4.4 mGuard delta anschließen

Klemmblock

Der Anschluss der **Versorgungsspannung** und des **Meldekontaktes** erfolgt über einen 6-poligen Klemmblock mit Schraubverriegelung.



⌦ Warnung!

Der mGuard ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsspannungsanschlüsse sowie an den Meldekontakt nur PELV-Spannungskreise oder wahlweise SELV-Spannungskreise mit den Spannungsbeschränkungen gemäß IEC/EN 60950 angeschlossen werden.

Betriebsspannung

NEC Class 2 power source 12VDC bzw. 24VDC -25% +33% Sicherheitskleinspannung (SELV/PELV, redundante Eingänge entkoppelt), max. 5A. Pufferzeit min. 10ms bei 24VDC.

Redundante Spannungsversorgung

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung den mGuard alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

Meldekontakt

Der Meldekontakt dient der Funktionsüberwachung des mGuard und ermöglicht damit eine Ferndiagnose. Über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) wird durch Kontaktunterbrechung Folgendes gemeldet:

- Der Ausfall mindestens einer der zwei Versorgungsspannungen.
- Eine dauerhafte Störung im mGuard (interne 3,3 VDC-Spannung, Versorgungsspannung 1 oder 2 < 9,6 V, …).
- Der fehlerhafte Linkstatus mindestens eines Ports. Die Meldung des Linkstatus kann beim mGuard pro Port über das Management maskiert werden. Im Lieferzustand erfolgt keine Verbindungsüberwachung.
- Fehler beim Selbsttest.

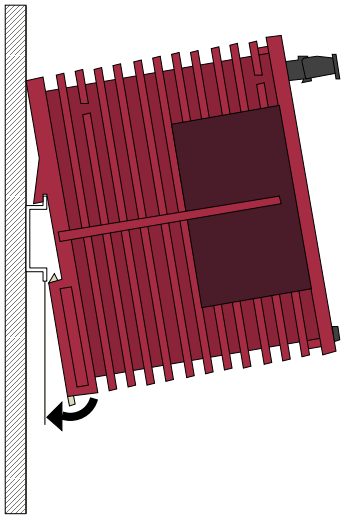
⌦ Bei nicht redundanter Zuführung der Versorgungsspannung meldet der mGuard den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen.

Erdungsanschluss

Zur Erdung des mGuard ist ein separater Schraubanschluss vorhanden.
Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für die Montage ist folgender Ablauf zweckmäßig:

- Ziehen Sie den Klemmblock vom mGuard ab und verdrahten Sie die Versorgungsspannungs- und Meldeleitungen.
- Montieren Sie den mGuard auf einer 35 mm Hutschiene nach DIN EN 50 022.

- Hängen Sie die obere Rastführung des mGuard in die Hutschiene ein und drücken Sie das mGuard dann nach unten gegen die Hutschiene, so dass es einrastet.
- Schließen Sie das Gerät an das lokale Netz oder den lokalen Rechner an, das/der geschützt werden soll (LAN).
- Über die Buchse zum Anschließen an das externe Netzwerk (WAN), z.B. Internet, den Anschluss am externen Netzwerk vornehmen. (Über dieses Netzwerk werden die Verbindungen zum entfernten Gerät bzw. entfernten Netz hergestellt.)



- ⌧ Die Erdung der Frontblende des Gehäuses des mGuard erfolgt über den Erdungsanschluss.
- ⌧ Das Gehäuse darf nicht geöffnet werden.
- ⌧ Die Schirmungsmasse der anschließbaren Industrial Twisted Pair-Leitungen ist elektrisch leitend mit der Frontblende verbunden.

Inbetriebnahme

Mit dem Anschluss der Versorgungsspannung über den 6-poligen Klemmblock nehmen Sie den mGuard in Betrieb. Verriegeln Sie den Klemmblock mit der seitlichen Verriegelungsschraube.

Netzwerkverbindung

Wenn Ihr Rechner bereits an einem Netzwerk angeschlossen ist, dann patchen Sie den mGuard *zwischen* die bereits bestehende Netzwerkverbindung.
Beachten Sie bitte, dass die Konfiguration zunächst nur über das LAN Interface erfolgen kann und die Firewall des mGuard allen IP Datenverkehr vom WAN zum LAN Interface unterbindet.

- ⌧ Es ist keine Treiber-Installation erforderlich.
- ⌧ Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern.
- ⌧ Beide Netzwerkschnittstellen des mGuard sind für den Anschluss an einen Rechner konfiguriert. Beim Anschluss an einen Hub ist Folgendes zu beachten: Bei deaktivierter *Autonegotiation* Funktion wird auch die Auto-MDIX Funktion deaktiviert, d. h. der Port des mGuard muss entweder an den Uplink-Port des Hub oder mittels eines Cross-Link-Kabels mit dem Hub verbunden werden.

Demontage

Um den mGuard von der Hutschiene zu demontieren, fahren Sie mit einem Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschie-

ber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen den mGuard nach oben.

4.5 mGuard PCI anschließen

4.5.1 Auswahl Treibermodus oder Power-over-PCI Modus

Treibermodus:
Der mGuard PCI kann wie eine normale Netzwerkkarte verwendet werden, die zusätzlich die mGuard Funktionen zur Verfügung stellt. In diesem Fall arbeitet der mGuard im Treibermodus und der mitgelieferte Treiber muss installiert werden. Der mGuard wird per Jumper auf den Treibermodus geschaltet.

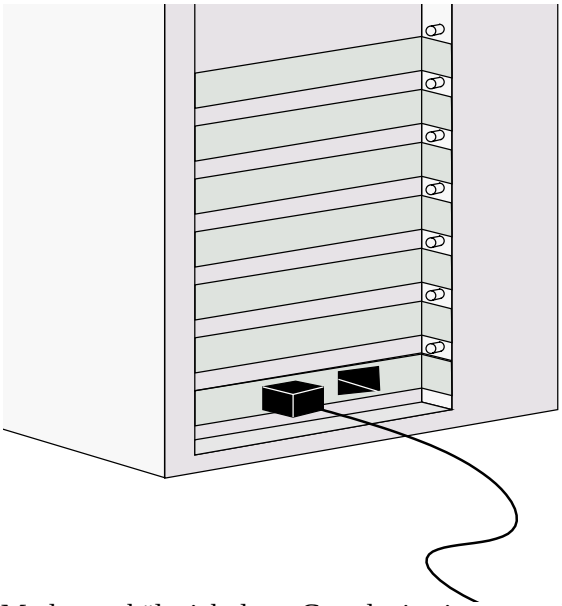
Power-over-PCI Modus:
Wenn die Netzwerkkarten-Funktionalität des mGuard nicht gebraucht wird oder nicht verwendet werden soll, kann der mGuard PCI hinter eine vorhandene Netzwerkkarte (des selben Rechners oder eines anderen) quasi wie ein mGuard Standalone-Gerät angeschlossen werden. Tatsächlich steckt der mGuard PCI in dieser Betriebsart nur deswegen im PCI-Slot eines Rechners, um mit Strom versorgt zu werden und ein Gehäuse zu haben. Diese Betriebsart des mGuard wird Power-over-PCI Modus genannt. Der mGuard wird per Jumper auf diese Betriebsart geschaltet. Ein Treiber wird nicht installiert.

Entscheiden Sie vor dem Einbau in Ihren PC, in welchem Modus Sie den mGuard PCI betreiben möchten.

Treibermodus

In diesem Modus muss später ein Treiber für die PCI Schnittstelle des mGuard PCI (verfügbar für Windows XP/2000 und Linux) auf dem Computer installiert werden. Im Treibermodus wird keine weitere Netzwerkkarte für den Computer benötigt.

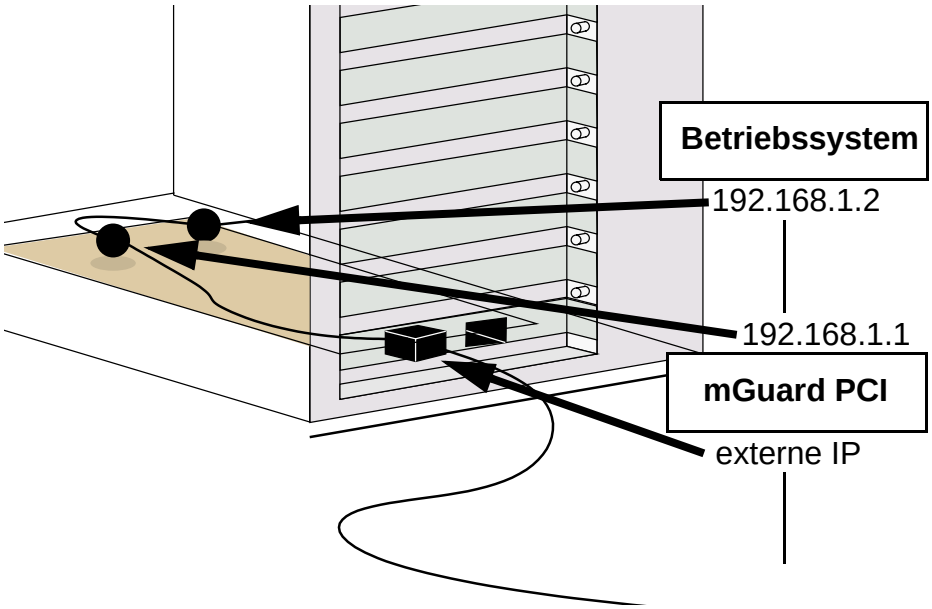
Stealth Modus im Treibermodus



Im *Stealth*-Modus verhält sich der mGuard wie eine normale Netzwerkkarte. Die IP-Adresse, die für die Netzwerk-Schnittstelle des Betriebssystems konfiguriert wird, übernimmt der mGuard auch für seine WAN-Schnittstelle. Somit tritt der mGuard für den Datenverkehr vom und zum Rechner als eigenes Gerät mit eigener Adresse gar nicht in Erscheinung.

⌦ Im Stealth Modus ist es nicht möglich PPPoE oder PPTP zu verwenden.

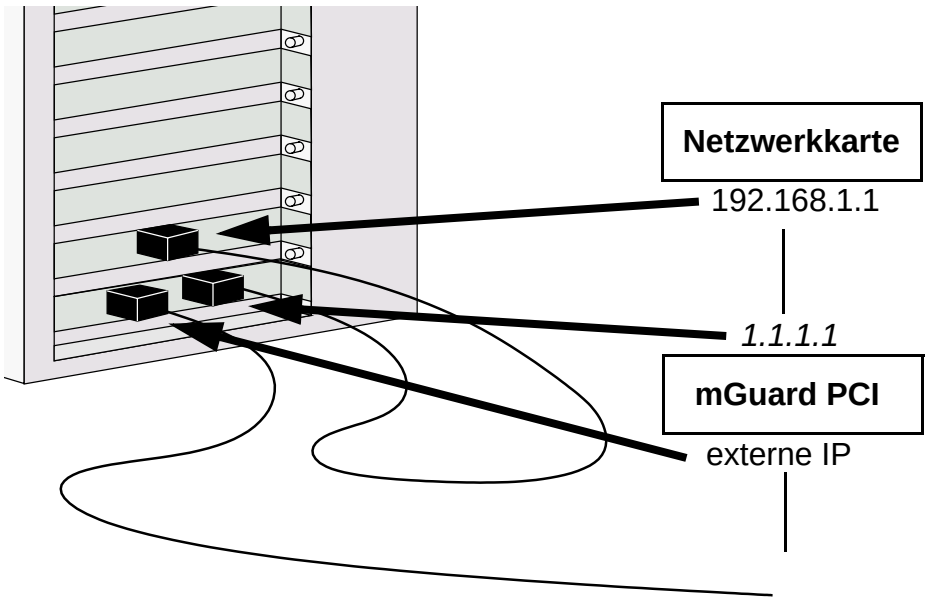
Router Modus im Treibermodus



Befindet sich der mGuard im *Router*-Modus (oder *PPPoE*- oder *PPTP*-Modus), bildet er mit dem Betriebssystem des Rechners, auf dem der mGuard installiert ist, quasi ein eigenes Netzwerk. Für die IP-Konfiguration der Netzwerk-Schnittstelle des Betriebssystems bedeutet das Folgendes: Dieser muss eine IP-Adresse zugewiesen werden, die sich von der internen IP-Adresse des mGuard (gemäß werksseitiger Voreinstellung 192.168.1.1) unterscheidet.
(Dieser Zusammenhang wird in der obiger Zeichnung durch zwei schwarze Kugeln verdeutlicht.)
Eine dritte IP-Adresse wird an der WAN Buchse des mGuard verwendet, mit der die Verbindung zu einem externen Netz (z. B. Internet) erfolgt.

Power-over-PCI Modus

Stealth Modus im Power-over-PCI Modus

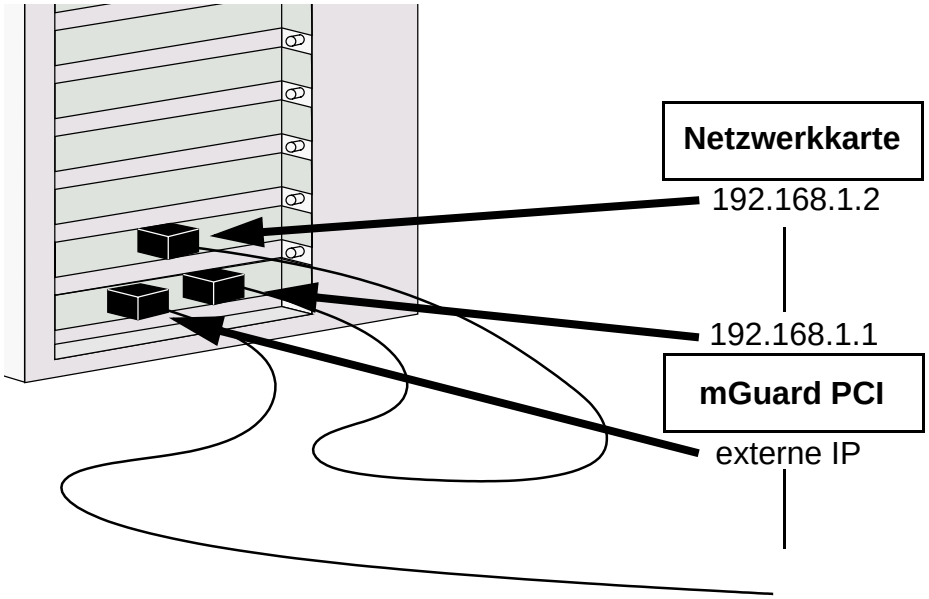


Im Power-over-PCI Modus wird für den mGuard PCI keine Treibersoftware installiert. An die LAN Ethernet Buchse (3) (Siehe “Einbau der Hardware” auf Seite 30.) des mGuard PCI wird eine weitere Netzwerkkarte angeschlossen, im gleichen oder einem anderen Computer.
Die IP-Adresse, die für die Netzwerk-Schnittstelle des Betriebssystems

konfiguriert wird, übernimmt der mGuard auch für seine WAN-Schnittstelle. Somit tritt der mGuard für den Datenverkehr vom und zum Rechner als eigenes Gerät mit eigener Adresse gar nicht in Erscheinung.

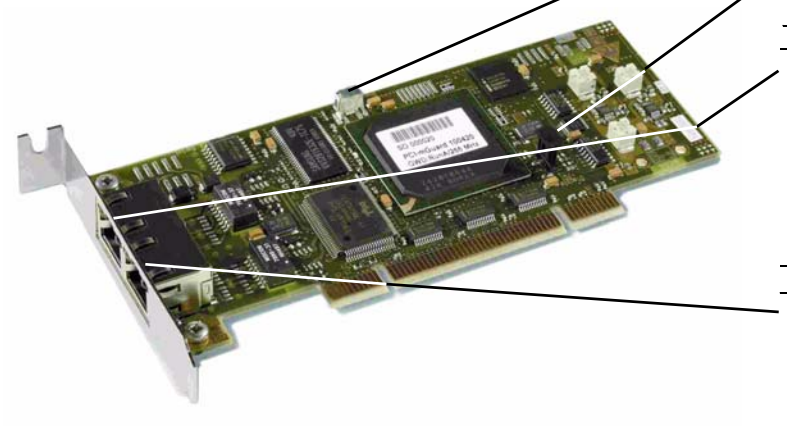
⌦ Im Stealth Modus ist es nicht möglich PPPoE oder PPTP zu verwenden.

Router Modus im Power-over-PCI-Modus



Befindet sich der mGuard im *Router*-Modus (oder *PPPoE* oder *PPTP* Modus), arbeiten der mGuard und die an seiner LAN-Buchse angeschlossene Netzwerkkarte - installiert im selben Rechner oder einem anderen - wie ein eigenes Netzwerk.
Für die IP-Konfiguration der Netzwerk-Schnittstelle des Betriebssystem des Rechners, in dem die Netzwerkkarte installiert ist, bedeutet das Folgendes:
Dieser Netzwerk-Schnittstelle muss eine IP-Adresse zugewiesen werden, die sich von der internen IP-Adresse des mGuard (gemäß werksseitiger Voreinstellung 192.168.1.1) unterscheidet.
Eine dritte IP-Adresse wird an der WAN Buchse des mGuard verwendet, mit der die Verbindung zu einem externen Netz (z. B. Internet) erfolgt.

4.5.2 Einbau der Hardware



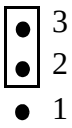
(1) Rescue Knopf

(2) Jumper zum Aktivieren/Deaktivieren des Treibermodus

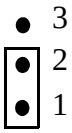
(3) LAN Ethernet Buchse (intern)
Ist im Treibermodus deaktiviert. Zum Anschluss eines anderen zu schützenden Computers/Netzwerks oder einer alternativen Netzwerkkarte

(4) WAN Ethernet Buchse (extern)
VPN Verbindungen werden über diese Schnittstelle aufgebaut. Gemäß Werkseinstellung sind hier eingehende Verbindungen gesperrt. Verwenden Sie ein UTP Kabel (CAT 5).

1. Konfigurieren Sie den mGuard für den Treibermodus oder Power-over-PCI Modus. (Siehe “Auswahl Treibermodus oder Power-over-PCI Modus” auf Seite 27.)
   Um den **Treibermodus** zu aktivieren, setzen Sie den Jumper (2) auf die folgende Position:

   Um den **Power-over-PCI Modus** zu aktivieren, setzen Sie den Jumper (2) auf die folgende Position:

2. Schalten Sie den Computer sowie andere angeschlossene Peripheriegeräte aus. Folgen Sie den Sicherheitshinweisen zur elektrostatischen Entladung.
3. Ziehen Sie das Stromkabel.
4. Öffnen Sie die Abdeckung des Computers. (Bitte folgenden Sie dabei der Beschreibung im Handbuch des Computers).
5. Wählen Sie einen freien PCI Steckplatz (3.3V oder 5V) für den mGuard PCI.
6. Entfernen Sie das dazugehörige Slotblech durch Lösen der entsprechenden Schraube und Herausziehen des Slotblechs. Bewahren Sie die Schraube für das Festschrauben der mGuard PCI Karte auf.
7. Richten Sie die Steckerleiste der mGuard PCI Karte vorsichtig über der Buchsenleiste des PCI Steckplatzes auf dem Motherboard aus, und drücken Sie anschließend die Karte gleichmäßig in die Buchsenleiste hinein.
8. Schrauben Sie die das Slotblech der Karte fest.
9. Schließen Sie die Abdeckung des Computers wieder.
10. Schließen Sie das Stromkabel des Computers wieder an und schalten Sie

diesen ein.

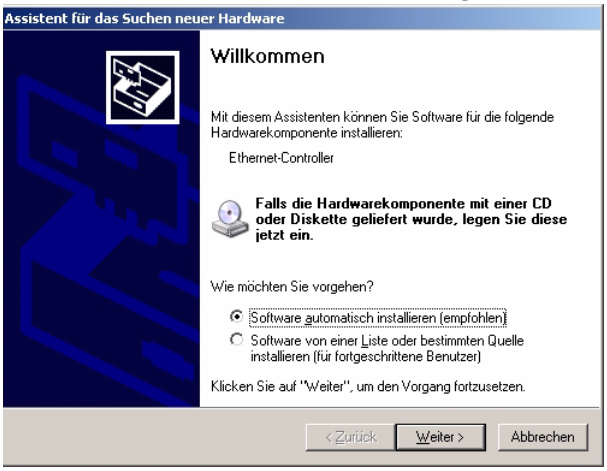
4.5.3 Treiber Installation

Windows XP

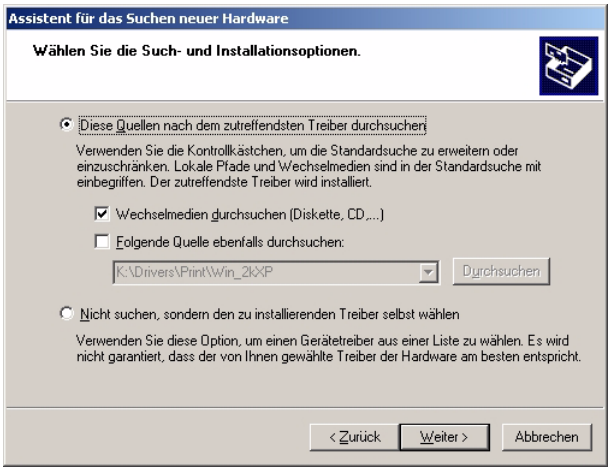
☞ Falls noch nicht geschehen, führen Sie die unter „Einbau der Hardware” auf Seite 30 beschriebenen Schritte aus.

⌦ Nur wenn der mGuard PCI im Treibermodus arbeitet, ist die Installation eines Treibers erforderlich und möglich (siehe „Treibermodus” auf Seite 27).

Um den Treiber zu installieren, schalten Sie den Computer ein, melden sich mit Administratorrechten an und warten dann, bis das folgende Fenster erscheint:


Assistent für das Suchen neuer Hardware
Willkommen
Mit diesem Assistenten können Sie Software für die folgende Hardwarekomponente installieren:
Ethernet-Controller
Falls die Hardwarekomponente mit einer CD oder Diskette geliefert wurde, legen Sie diese jetzt ein.
Wie möchten Sie vorgehen?
Software automatisch installieren (empfohlen)
Software von einer Liste oder bestimmten Quelle installieren (für fortgeschrittene Benutzer)
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.
< Zurück
Weiter >
Abbrechen

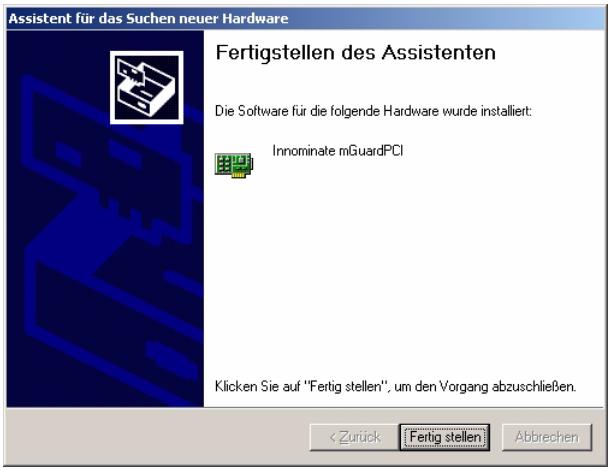
1. Wählen Sie **Software von einer Liste oder bestimmten Quelle installieren (für fortgeschrittene Benutzer)** und klicken Sie auf **Weiter**


Assistent für das Suchen neuer Hardware
Wählen Sie die Such- und Installationsoptionen.
Diese Quellen nach dem zutreffendsten Treiber durchsuchen
Verwenden Sie die Kontrollkästchen, um die Standardsuche zu erweitern oder einzuschränken. Lokale Pfade und Wechselmedien sind in der Standardsuche mit einbegriffen. Der zutreffendste Treiber wird installiert.
Wechselmedien durchsuchen (Diskette, CD,...)
Folgende Quelle ebenfalls durchsuchen:
K:\Drivers\Print\Win_2kXP
Durchsuchen
Nicht suchen, sondern den zu installierenden Treiber selbst wählen
Verwenden Sie diese Option, um einen Gerätetreiber aus einer Liste zu wählen. Es wird nicht garantiert, dass der von Ihnen gewählte Treiber der Hardware am besten entspricht.
< Zurück
Weiter >
Abbrechen

2. Klicken Sie auf **Weiter**

Hardwareinstallation
Die Software, die für diese Hardware installiert wird:
Innominate mGuardPCI
hat den Windows-Logo-Test nicht bestanden, der die Kompatibilität mit Windows XP überprüft. (Warum ist dieser Test wichtig?)
Das Fortsetzen der Installation dieser Software kann die korrekte Funktion des Systems direkt oder in Zukunft beeinträchtigen. Microsoft empfiehlt strengstens, die Installation jetzt abzubrechen und sich mit dem Hardwarehersteller für Software, die den Windows-Logo-Test bestanden hat, in Verbindung zu setzen.
Installation fortsetzen
Installation abbrechen

3. Klicken Sie auf **Installation fortsetzen**


Assistent für das Suchen neuer Hardware
Fertigstellen des Assistenten
Die Software für die folgende Hardware wurde installiert:
Innominate mGuardPCI
Klicken Sie auf "Fertig stellen", um den Vorgang abzuschließen.
< Zurück
Fertig stellen
Abbrechen

4. Klicken Sie auf **Fertig stellen**

Windows 2000

☞ Falls noch nicht geschehen, führen Sie die unter „Einbau der Hardware” auf Seite 30 beschriebenen Schritte aus.

☞ Die folgenden Abbildungen zeigen die englische Version von Windows 2000.

⌧ Nur wenn der mGuard PCI im Treibermodus arbeitet, ist die Installation eines Treibers erforderlich und möglich (siehe „Treibermodus” auf Seite 27).

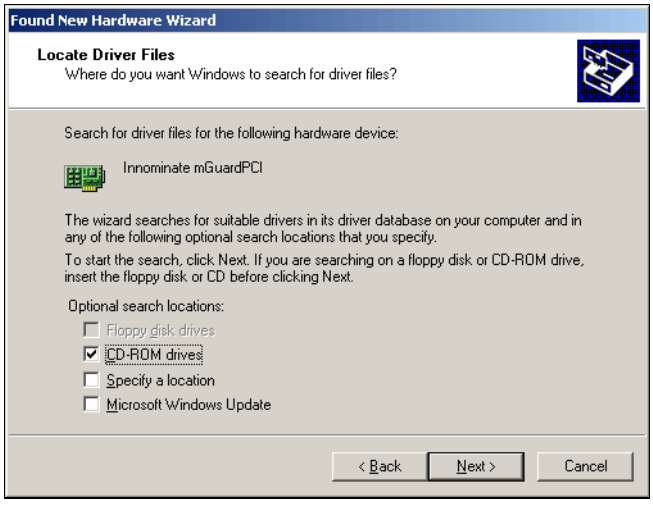
Warten Sie, bis nach Einschalten des Computers und nach dem Anmelden das folgende Fenster erscheint:

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
This wizard helps you install a device driver for a hardware device.
To continue, click Next.
< Back
Next >
Cancel

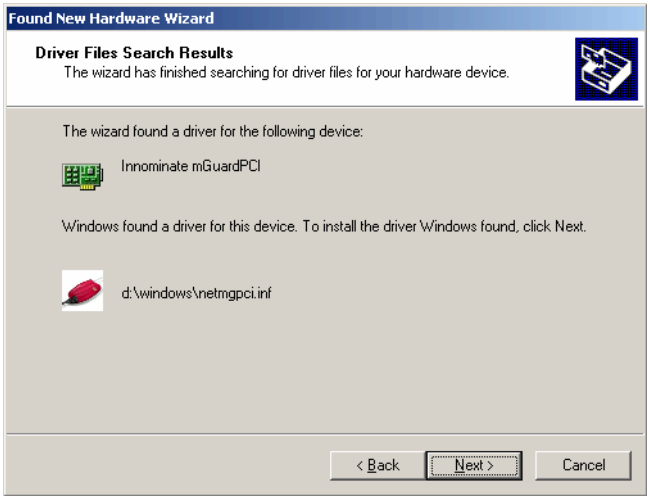
1. Klicken Sie auf **Weiter**

Found New Hardware Wizard
Install Hardware Device Drivers
A device driver is a software program that enables a hardware device to work with an operating system.
This wizard will complete the installation for this device:
Innominate mGuardPCI
A device driver is a software program that makes a hardware device work. Windows needs driver files for your new device. To locate driver files and complete the installation click Next.
What do you want the wizard to do?
Search for a suitable driver for my device (recommended)
Display a list of the known drivers for this device so that I can choose a specific driver
< Back
Next >
Cancel

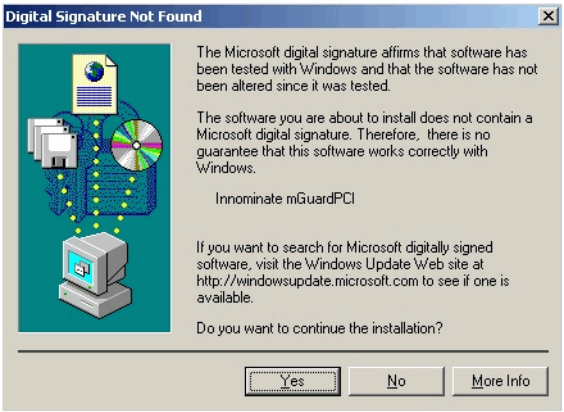
2. Wählen Sie **Suche nach einem passenden Treiber für das Gerät** und klicken Sie auf **Weiter**


Found New Hardware Wizard
Locate Driver Files
Where do you want Windows to search for driver files?
Search for driver files for the following hardware device:
Innominate mGuardPCI
The wizard searches for suitable drivers in its driver database on your computer and in any of the following optional search locations that you specify.
To start the search, click Next. If you are searching on a floppy disk or CD-ROM drive, insert the floppy disk or CD before clicking Next.
Optional search locations:
Floppy disk drives
CD-ROM drives
Specify a location
Microsoft Windows Update
< Back
Next >
Cancel

3. Wählen Sie **CD-ROM Laufwerke** und klicken Sie auf **Weiter**


Found New Hardware Wizard
Driver Files Search Results
The wizard has finished searching for driver files for your hardware device.
The wizard found a driver for the following device:
Innominate mGuardPCI
Windows found a driver for this device. To install the driver Windows found, click Next.
d:\windows\netmgpci.inf
< Back
Next >
Cancel

4. Klicken Sie auf **Weiter**


Digital Signature Not Found
The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.
The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.
Innominate mGuardPCI
If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.
Do you want to continue the installation?
Yes
No
More Info

5. Klicken Sie auf **Ja**

6. Klicken Sie auf **Fertigstellen**

Linux

Der Linuxtreiber ist im Sourcecode verfügbar und muss vor Verwendung übersetzt werden:

- Bauen und übersetzen Sie zunächst den Linuxkernel (2.4.25) im Verzeichnis **/usr/src/linux**
- Entpacken Sie die Treiber von der CD im Verzeichnis **/usr/src/pci-driver**

- Führen Sie die folgenden Kommandos aus
    - **cd /usr/src/pci-driver**
    - **make LINUXDIR=/usr/src/linux**
    - **install -m0644 mguard.o /lib/modules/2.4.25/kernel/drivers/net/**
    - **depmod -a**
- Der Treiber kann nun mit dem folgenden Kommando geladen werden
    - **modprobe mguard**

4.6 mGuard smart anschließen

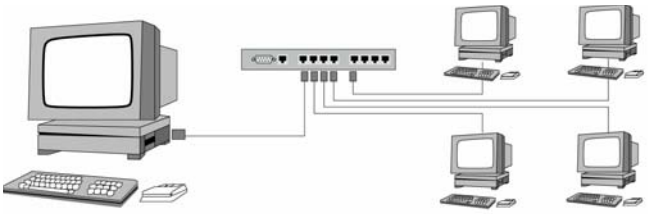
Ethernet-Stecker zum direkten Anschließen an das zu schützende Gerät bzw. Netz (**lokales** Gerät oder Netz).

USB-Stecker zum Anschließen an die USB-Schnittstelle eines Rechners.
Dient nur zur Stromversorgung!

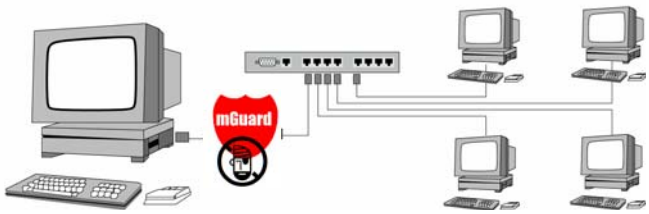
Buchse zum Anschließen an das externe Netzwerk, z. B. WAN, Internet.
(Über dieses Netz werden die Verbindungen zum entfernten Gerät bzw. Netz hergestellt.)
Benutzen Sie ein UTP-Kabel (CAT 5).

Wenn Ihr Rechner bereits an einem Netzwerk angeschlossen ist, dann stekken Sie den mGuard zwischen Netzwerk-Interface des Rechners und Netzwerk.

vorher:



nachher:



⌦ Es ist keine Treiber-Installation erforderlich.

⌦ Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern.

5 Konfiguration vorbereiten

5.1 Anschließen des mGuards

mGuard blade

- Der mGuard blade muss in der mGuard bladeBase montiert sein, und mindestens eines der Netzteile der bladeBase muss in Betrieb sein.
- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  – an der LAN-Buchse des mGuard angeschlossen sein,
  – oder der Rechner muss über das Netzwerk mit dem mGuard verbunden sein.
- Bei Fernkonfiguration: Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d.h. die erforderlichen Verbindungen müssen funktionieren.

mGuard delta

- mGuard delta: Der mGuard muss an seine Stromversorgung angeschlossen sein.
- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  – am LAN Switch (Ethernetbuchse 4 bis 7) des mGuard angeschlossen sein,
  – oder er muss über das lokale Netzerk mit dem mGuard verbunden sein.
- Bei Fernkonfiguration: Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d.h. die erforderlichen Verbindungen müssen funktionieren.

mGuard industrial

- mGuard industrial: Der mGuard muss an mindestens ein aktives Netzteil angeschlossen sein.
- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  – an der LAN-Buchse des mGuard angeschlossen sein,
  – oder der Rechner muss über das Netzwerk mit dem mGuard verbunden sein.
- Bei Fernkonfiguration: Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d.h. die erforderlichen Verbindungen müssen funktionieren.

mGuard smart

- mGuard smart: Der mGuard muss eingeschaltet sein, d. h. per USB-Kabel an einen eingeschalteten Rechner (oder Netzteil) angeschlossen sein, so dass er mit Strom versorgt wird.
- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  – am Ethernet-Stecker des mGuard angeschlossen sein,
  – oder er muss über das lokale Netzerk mit ihm verbunden sein.
- Bei Fernkonfiguration: Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d.h. die erforderlichen Verbindungen müssen funktionieren.

mGuard PCI

- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  – die mGuard PCI Treiber installiert haben, falls der der mGuard im Treibermodus betrieben wird oder

– über die LAN- Ethernetverbindung angeschlossen sein, falls der mGuard im Power-over-PCI Modus betrieben wird.
- Bei Fernkonfiguration: Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d.h. die erforderlichen Verbindungen müssen funktionieren.

5.2 Lokale Konfiguration: Bei Inbetriebnahme

Der mGuard wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird (z. B. MS Internet-Explorer ab Version 5.0, Mozilla Firefox ab Version 1.5, Safari oder w3m.)

⌧ Der Web-Browser muss SSL (d. h. https) unterstützen.

Der mGuard ist gemäß Werkseinstellung unter folgender Adressen erreichbar:

Werkseinstellung:

Stealth-Modus: (Auslieferungszustand bis auf mGuard delta)	https://1.1.1.1/
Router-Modus: (Auslieferungszustand mGuard delta)	https://192.168.1.1/

5.2.1 mGuard blade, industrial und smart

Bei konfigurierter Netzwerk-Schnittstelle

Damit der mGuard über die Adresse https://1.1.1.1/ angesprochen werden kann, muss er an eine konfigurierte Netzwerk-Schnittstelle angeschlossen sein. Das ist der Fall, wenn man ihn zwischen eine bestehende Netzwerkverbindung steckt - siehe Abbildung im Abschnitt

- „mGuard blade anschließen“ auf Seite 21,
- „mGuard industrial anschließen“ auf Seite 23 oder
- „mGuard smart anschließen“ auf Seite 36.

In diesem Fall wird der Web-Browser nach Eingabe der Adresse https://1.1.1.1/ die Verbindung zur Konfigurations-Oberfläche des mGuard herstellen - siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 42. Fahren Sie in diesem Falle dort fort.

Bei nicht konfigurierter Netzwerk-Schnittstelle

Falls die Netzwerk-Schnittstelle des Rechners nicht konfiguriert ist...

Wenn der Konfigurations-Rechner noch nicht an einem Netzwerk angeschlossen war, z. B. weil der Rechner neu ist, dann ist seine Netzwerk-Schnittstelle im Allgemeinen nicht konfiguriert. Das heißt der Rechner „weiß“ noch nicht, dass der Netzwerkverkehr über diese Schnittstelle läuft.

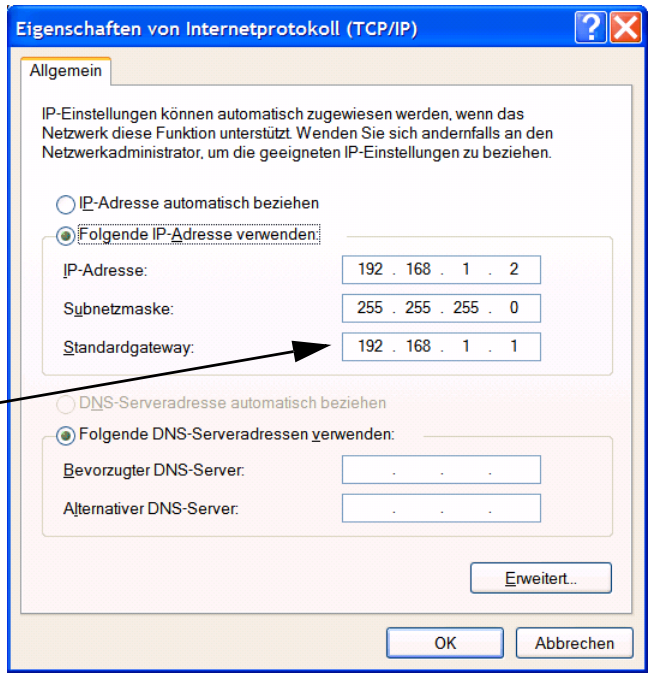
In diesem Fall müssen Sie das Standardgateway initialisieren, indem Sie ihm einen Dummy-Wert zuweisen. Gehen Sie dazu wie folgt vor:

Standardgateway initialisieren

1. Ermitteln Sie die zurzeit gültige Standardgateway-Adresse. Unter Windows XP gehen Sie dazu wie folgt vor:
   – **Start, Systemsteuerung, Netzwerkverbindungen** klicken.
   – Das Symbol des LAN-Adapters mit der rechten Maustaste klicken, so dass sich das Kontextmenü öffnet. Im Kontextmenü **Eigenschaften** klicken.
   – Im Dialogfeld *Eigenschaften von LAN-Verbindung lokales Netz* auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag **Internetprotokoll (TCP/IP)** markieren. Dann die

Schaltfläche **Eigenschaften** klicken, so dass folgendes Dialogfenster angezeigt wird:

Hier die IP-Adresse des Standardgateway nachschlagen oder festlegen.


Eigenschaften von Internetprotokoll (TCP/IP)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 1 . 2
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: 192 . 168 . 1 . 1
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server:
Alternativer DNS-Server:
Erweitert...
OK
Abbrechen

Falls in diesem Dialogfeld keine IP-Adresse des Standardgateway angegeben ist, z. B. weil *IP-Adresse automatisch beziehen* aktiviert ist, dann geben Sie eine IP-Adressen manuell ein. Dazu aktivieren Sie zunächst **Folgende IP-Adressen verwenden** und geben dann zum Beispiel folgende Adressen ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standardgateway:	192.168.1.1

⌦ Auf keinen Fall dem Konfigurations-Rechner eine Adresse wie 1.1.1.2 geben!

2. Auf DOS-Ebene (Menü **Start, Alle Programme, Zubehör, Eingabeaufforderung**) geben Sie ein:
   `arp -s` <IP des Standardgateway> **`aa-aa-aa-aa-aa-aa`**
   Beispiel:
   Sie haben als Standardgateway-Adresse ermittelt oder festgelegt: 192.168.1.1
   Dann lautet der Befehl:
   `arp -s 192.168.1.1 aa-aa-aa-aa-aa-aa`

3. Zur Konfiguration stellen Sie jetzt die Konfigurationsverbindung her - siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 42

4. Nach der Konfiguration stellen Sie das Standardgateway wieder zurück. Dazu entweder den Konfigurations-Rechner neu starten oder auf DOS-Ebene folgendes Kommando eingeben:
   `arp -d`

⌦ Je nach dem, wie Sie den mGuard konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

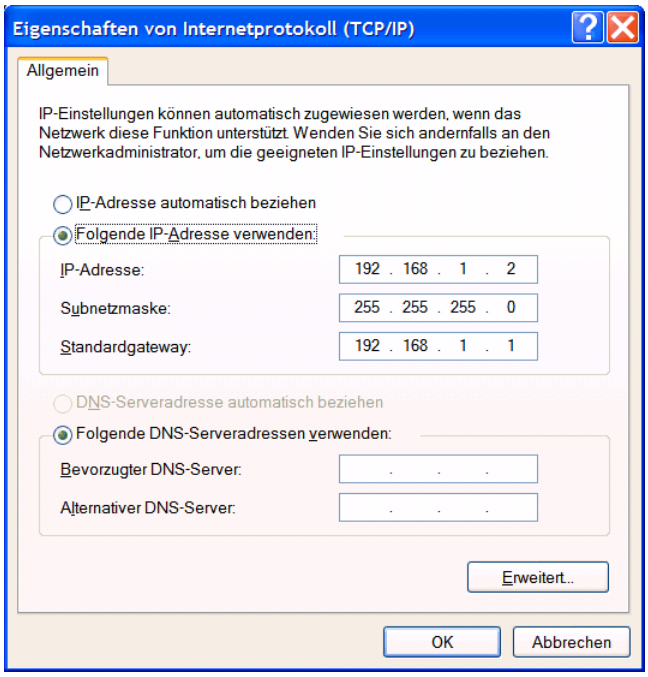
5.2.2 mGuard delta

Bei Auslieferung oder nach Zurücksetzen auf die Werkseinstellung oder Flashen des mGuards ist der mGuard über die LAN Schnittstellen 4 bis 7 unter der IP

Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar. Für einen Zugriff auf die Konfigurationsoberfläche kann es daher nötig sein, die Konfiguration Ihres Computer anzupassen.

Unter Windows XP gehen Sie dazu wie folgt vor:

– **Start, Systemsteuerung, Netzwerkverbindungen** klicken.
– Das Symbol des LAN-Adapters mit der rechten Maustaste klicken, so dass sich das Kontextmenü öffnet. Im Kontextmenü **Eigenschaften** klicken.
– Im Dialogfeld *Eigenschaften von LAN-Verbindung lokales Netz* auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag **Internetprotokoll (TCP/IP)** markieren. Dann die Schaltfläche **Eigenschaften** klicken, so dass folgendes Dialogfenster angezeigt wird::


Eigenschaften von Internetprotokoll (TCP/IP)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 1 . 2
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: 192 . 168 . 1 . 1
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server:
Alternativer DNS-Server:
Erweitert...
OK
Abbrechen

Aktivieren Sie zunächst **Folgende IP-Adressen verwenden** und geben dann zum Beispiel folgende Adressen ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standardgateway:	192.168.1.1

⌦ Je nach dem, wie Sie den mGuard konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

5.2.3 mGuard PCI

Installieren der mGuard Karte

Wenn Sie die mGuard Karte noch nicht in ihrem Computer installiert haben, folgen Sie bitte zunächst den unter „Einbau der Hardware“ auf Seite 30 beschriebenen Schritten.

Installieren der mGuard Treiber

Wenn Sie den mGuard für den Treiber Modus konfiguriert haben, stellen Sie bitte sicher, dass die Treiber wie unter „Treiber Installation“ auf Seite 31 beschrieben installiert sind.

Konfiguration der Netzwerk-Schnittstelle

Wenn Sie den mGuard

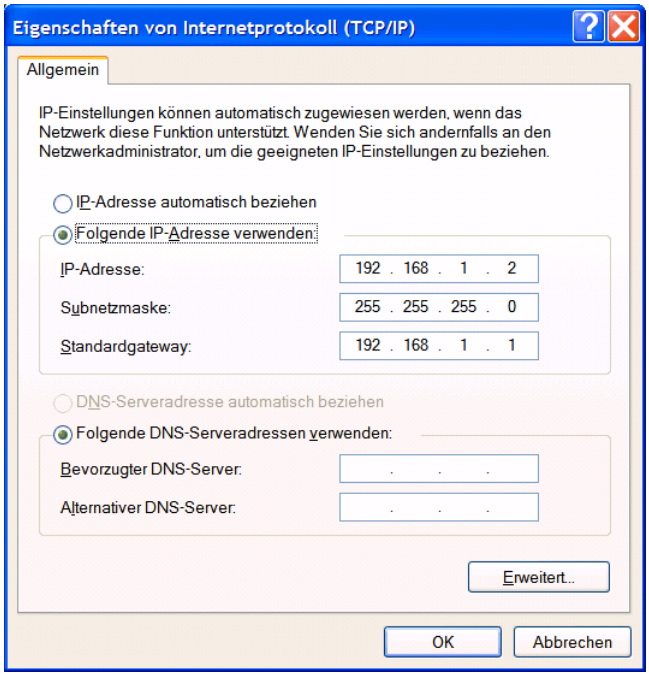
- im Treiber Modus betreiben und die Netzwerk-Schnittstelle des mGuards für das Betriebssystem noch nicht konfiguriert wurde oder
- im Power-over-PCI Modus betrieben und die Netzwerk-Schnittstelle des am

LAN Interface des mGuards angeschlossenen Computers noch nicht konfiguriert wurde

dann müssen Sie diese konfigurieren bevor Sie die Sicherheitseigenschaften des mGuards konfigurieren können.

Unter Windows XP gehen konfigurieren Sie die Netzwerk-Schnittstelle wie folgt:

– **Start, Systemsteuerung, Netzwerkverbindungen** klicken.
– Das Symbol des LAN-Adapters mit der rechten Maustaste klicken, so dass sich das Kontextmenü öffnet. Im Kontextmenü **Eigenschaften** klicken.
– Im Dialogfeld *Eigenschaften von LAN-Verbindung lokales Netz* auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag **Internetprotokoll (TCP/IP)** markieren. Dann die Schaltfläche **Eigenschaften** klicken, so dass folgendes Dialogfenster angezeigt wird:


Eigenschaften von Internetprotokoll (TCP/IP)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 1 . 2
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: 192 . 168 . 1 . 1
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server:
Alternativer DNS-Server:
Erweitert...
OK
Abbrechen

Standardgateway

Nachdem Sie die Netzwerk-Schnittstelle konfiguriert haben, sollten Sie die Konfigurationsoberfläche des mGuards mit einem Webbrowser unter der URL „https://1.1.1.1/“ erreichen können. Wenn dies nicht möglich ist, dann ist möglicherweise das Standardgateway ihres Computers nicht erreichbar. In diesem Fall muß es ihrem Computer wie folgt vorgetäuscht werden:

Standardgateway initialisieren

1. Ermitteln Sie die zurzeit gültige Standardgateway-Adresse.
   Unter Windows XP folgen Sie dazu den oben unter „Installieren der mGuard Karte“ beschriebenen Schritten, um das Dialogfeld **Eigenschaften von Internetprotokoll (TCP/IP)** zu öffnen.
   Falls in diesem Dialogfeld keine IP-Adresse des Standardgateway angegeben ist, z. B. weil *IP-Adresse automatisch beziehen* aktiviert ist, dann geben Sie eine IP-Adressen manuell ein. Dazu aktivieren Sie zunächst **Folgende IP-Adressen verwenden** und geben dann zum Beispiel folgende Adressen ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standardgateway:	192.168.1.1

⌦ Auf keinen Fall dem Konfigurations-Rechner eine Adresse wie 1.1.1.2 geben!

2. Auf DOS-Ebene (Menü **Start, Alle Programme, Zubehör, Eingabeaufforderung**) geben Sie ein:
   `arp -s` <IP des Standardgateway> **`aa-aa-aa-aa-aa-aa`**
   Beispiel:
   Sie haben als Standardgateway-Adresse ermittelt oder festgelegt: 192.168.1.1
   Dann lautet der Befehl:
   `arp -s 192.168.1.1 aa-aa-aa-aa-aa-aa`

3. Zur Konfiguration stellen Sie jetzt die Konfigurationsverbindung her - siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 42

4. Nach der Konfiguration stellen Sie das Standardgateway wieder zurück. Dazu entweder den Konfigurations-Rechner neu starten oder auf DOS-Ebene folgendes Kommando eingeben:
   `arp -d`

⌦ Je nach dem, wie Sie den mGuard konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

5.3 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Der mGuard wird per Web-Browser (z. B. Firefox, MS Internet-Explorer oder Safari) konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.
⌦ **Der Web-Browser muss SSL (d. h. https) unterstützen.**
Der mGuard wird je nach Modell entweder im Netzwerk-Modus ***Stealth*** oder ***Router*** ausgeliefert und ist dem entsprechend unter einer der folgenden Adressen erreichbar:

Werkseinstellung:

Stealth-Modus	https://1.1.1.1/
Router- / PPPoE- / PPPT-Modus:	https://192.168.1.1/

Gehen Sie wie folgt vor:

1. Starten Sie einen Web-Browser.
   (Z. B. Firefox, MS Internet-Explorer oder Safari; der Web-Browser muss SSL (d. h. https) unterstützen.)
2. Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum mGuard erschwert werden könnte.
   Im MS Internet Explorer nehmen Sie diese Einstellung wie folgt vor: Menü **Extras, Internetoptionen...**, Registerkarte *Verbindungen*:
   Unter *DFÜ- und VPN-Einstellungen* muss **Keine Verbindung wählen** aktiviert sein.
3. In der Adresszeile des Web-Browsers geben Sie die Adresse des mGuard vollständig ein.
   Im **Stealth**-Modus (= Werkseinstellung außer mGuard delta) lautet diese immer

   `https://1.1.1.1/`

IP-Adresse des mGuard im *Stealth*-Modus:
https://1.1.1.1/

wenn nicht im *Stealth*-Modus:
https://192.168.1.1/

und in den Betriebsarten **Router** (= Werkseinstellung mGuard delta), **PPPoE** oder **PPTP** lautet diese immer

`https://192.168.1.1/`

Folge:
Sie gelangen zur Administrator-Website des mGuard. Der auf der nächsten Seite abgebildete Sicherheitshinweis erscheint.

⌦ Falls Sie die konfigurierte Adresse vergessen haben:

Falls die Adresse des mGuard im *Router- PPPoE-* oder *PPTP*-Modus auf einen anderen Wert gesetzt ist und Sie kennen die aktuelle Adresse nicht, dann müssen Sie den mGuard mit Hilfe der **Recovery**-Taste in den Stealth-Modus (mGuard delta: Router-Modus) stellen und damit auf folgende Adresse: https://1.1.1.1/ (siehe „Recovery-Prozedur ausführen“ auf Seite 142).

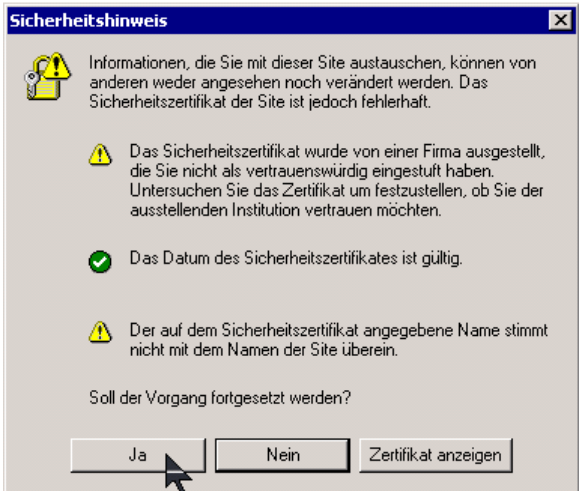
⌦ Falls die Administrator-Website nicht angezeigt wird...

Sollte auch nach wiederholtem Versuch der Web-Browser melden, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Prüfen Sie, ob der Standardgateway des angeschlossenen Konfigurations-Rechners initialisiert ist. Siehe „Lokale Konfiguration: Bei Inbetriebnahme“ auf Seite 38
- Eine bestehende Firewall gegebenenfalls deaktivieren.
- Achten Sie darauf, dass der Browser keinen Proxy Server verwendet.
  Im MS Internet Explorer (Version 6.0) nehmen Sie diese Einstellung wie folgt vor: Menü **Extras, Internetoptionen...**, Registerkarte *Verbindungen*: Unter *LAN-Einstellungen* auf die Schaltfläche **Einstellungen...** klicken, im Dialogfeld *Einstellungen für lokales Netzwerk (LAN)* dafür sorgen, dass unter Proxyserver der Eintrag **Proxyserver für LAN verwenden** nicht aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Unter Windows Menü **Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen** bzw. **Netzwerk- und DFÜ-Verbindungen** das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü **Deaktivieren** wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint dieser Sicherheitshinweis (MS Internet-Explorer):


Sicherheitshinweis
Informationen, die Sie mit dieser Site austauschen, können von anderen weder angesehen noch verändert werden. Das Sicherheitszertifikat der Site ist jedoch fehlerhaft.
Das Sicherheitszertifikat wurde von einer Firma ausgestellt, die Sie nicht als vertrauenswürdig eingestuft haben. Untersuchen Sie das Zertifikat um festzustellen, ob Sie der ausstellenden Institution vertrauen möchten.
Das Datum des Sicherheitszertifikates ist gültig.
Der auf dem Sicherheitszertifikat angegebene Name stimmt nicht mit dem Namen der Site überein.
Soll der Vorgang fortgesetzt werden?
Ja
Nein
Zertifikat anzeigen

Erläuterung:
Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

Quittieren Sie den entsprechenden Sicherheitshinweis mit **Ja**.

Folge:
Nach Abfrage des Benutzernamens (Login) und Passwortes wird die Administrator-Website des mGuard angezeigt.
Werksseitig ist voreingestellt:

Login: `admin`
Passwort: `mGuard`

⌧ Groß- und Kleinschreibung beachten!

Zur Konfiguration machen Sie auf den einzelnen Seiten der mGuard-Website die gewünschten bzw. erforderlichen Angaben.
Siehe „Konfiguration“ auf Seite 45.

⌧ Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern - siehe „Benutzerauthentifizierung →Lokale Benutzer“ auf Seite 95 .

5.4 Fernkonfiguration

Voraussetzung

Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

⌧ Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Um die Möglichkeit zur Fernkonfiguration einzuschalten, siehe Abschnitt „Verwaltung →Web Einstellungen“, „Zugriff“ auf Seite 54.

Fernkonfiguration

Um von einem entfernten Rechner aus den mGuard zu konfigurieren, stellen Sie von dort die Verbindung zum lokalen mGuard her.
Gehen Sie wie folgt vor:

1. Starten Sie dazu auf dem entfernten Rechner den Web-Browser (z. B.Firefox, MS Internet-Explorer oder Safari; der Web-Browser muss SSL (d. h. https) unterstützen.)
2. Als Adresse geben Sie an: Die IP-Adresse, unter der der mGuard von extern über das Internet bzw. WAN erreichbar ist, gegebenenfalls zusätzlich die Port-Nummer.

   Beispiel:
   Ist dieser mGuard über die Adresse 123.456.789.21 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 443 festgelegt, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: 123.456.789.21
   Bei einer anderen Port-Nummer ist diese hinter der IP-Adresse anzugeben, z. B.: 123.456.789.21:442

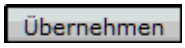
Zur Konfiguration machen Sie auf den einzelnen Seiten der mGuard-Website die gewünschten bzw. erforderlichen Angaben.
Siehe „Konfiguration“ auf Seite 45.

6 Konfiguration

6.1 Bedienung

Bildschirmaufteilung

1. Über das Menü links die Seite mit den gewünschten Einstellmöglichkeiten anklicken, z. B. *Verwaltung* → *Lizensierung*. Dann wird im Hauptfenster die Seite angezeigt - in Form einer Registerkarte - auf der Sie Einstellungen vornehmen können. Gegebenfalls gliedert sich eine Seiten in mehrere Registerkarten, zwischen denen Sie durch Klicken oben auf die Registerkartenzunge (auch *Tab* genannt) blättern können.
2. Auf der betreffenden Seite bzw. Registerkarte die gewünschten Einträge machen. Siehe dazu auch den nachfolgenden Unterabschnitt „Arbeiten mit Tabellen“ auf Seite 45.
3. Damit die Einstellungen vom Gerät übernommen werden, die Schaltfläche **Übernehmen** klicken.



Nach der Übernahme vom System erhalten Sie eine (bestätigende) Rückmeldung. Damit sind die neuen Einstellungen in Kraft. Sie bleiben in Kraft auch nach einem Neustart (Reset).

Arbeiten mit Tabellen

Viele Einstellungen werden als Datensätze gespeichert. Entsprechend werden Ihnen die einstellbaren Parameter und deren Werte in Form von Tabellenzeilen präsentiert. Sind mehrere Datensätze mit Einstellungen gesetzt (z. B. Firewall-Regeln), werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt bzw. abgearbeitet. Gegebenenfalls ist also auf die Reihenfolge der Einträge zu achten. Durch das Verschieben von Tabellenzeilen nach unten oder oben kann die Reihenfolge geändert werden.

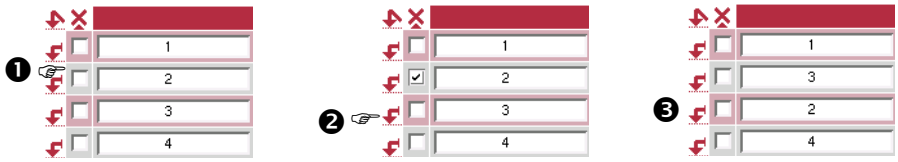
Bei Tabellen können Sie
– Zeilen einfügen, um einen neuen Datensatz mit Einstellungen anzulegen (z. B. die Firewall-Einstellungen für eine bestimmte Verbindung)
– Zeilen verschieben (d. h. umsortieren) und
– Zeilen löschen, um den gesamten Datensatz zu löschen.

Einfügen von Zeilen

1. Klicken Sie auf den Pfeil, unter dem Sie eine neue Zeile einfügen wollen:

2. Die neue Zeile ist eingefügt.

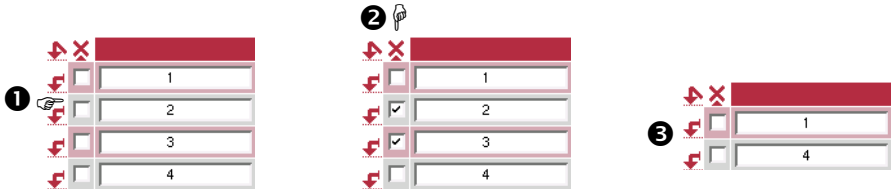
Verschieben von Zeilen



1. Markieren Sie eine oder mehrere Zeilen, die Sie verschieben wollen.
2. Klicken Sie auf den Pfeil, unter den Sie die markierten Zeilen verschieben wollen:

3. Die Zeilen sind verschoben.

Löschen von Zeilen



1. Markieren Sie die Zeilen, die Sie löschen wollen.
2. Klicken Sie auf das Zeichen zum Löschen:

3. Die Zeilen sind gelöscht.

Weitere Bedienhinweise

- Sollte bei erneuter Anzeige einer Seite diese nicht aktuell sein, weil der Browser sie aus dem Cache lädt, aktualisieren Sie die Anzeige der Seite. Dazu in der Browser-Symbolleiste das Symbol zum Aktualisieren klicken.
- Je nach dem, wie Sie den mGuard konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

Folgende Schaltflächen stehen auf dem Seitenkopf auf allen Seiten zur Verfügung:

Logout	Zum Abmelden nach einem Konfigurations-Zugriff auf den mGuard. Führt der Benutzer kein Logout durch, wird ein Logout automatisch durchgeführt, sobald keine Aktivität mehr stattfindet und die durch Timeout festgelegte Zeit abgelaufen ist. Ein erneuter Zugriff kann dann nur durch erneutes Anmelden (Login) erfolgen.

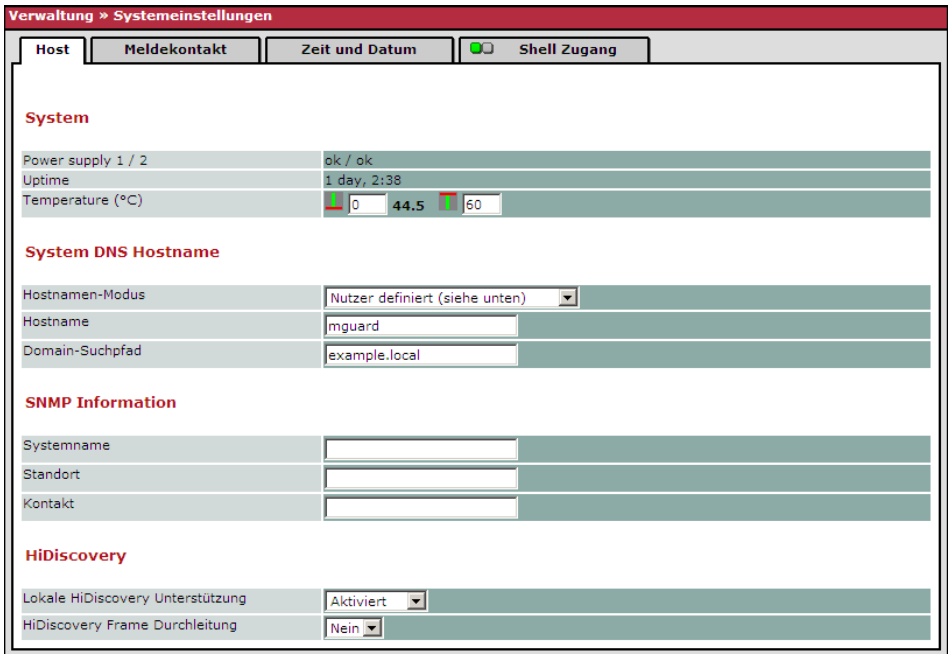
 Reset	Optionale Schaltfläche. Zurücksetzen auf die alten Werte. Wenn Sie auf einer Konfigurationsseite Werte eingetragen haben und diese noch nicht mit **Übernehmen** in Kraft gesetzt haben, können Sie mit **Reset** die Seite auf die alten Werte zurücksetzen. Diese Schaltfläche ist nur dann im Kopfbereich der Seite eingeblendet, wenn der Gültigkeitsbereich der **Übernehmen**-Schaltfläche auf *seitenübergreifend* gestellt ist - siehe „Verwaltung →Web Einstellungen“ auf Seite 54.
 Apply	Optionale Schaltfläche. Wirkt wie die Schaltfläche **Übernehmen** (s. o.), gilt aber seitenübergreifend. Diese Schaltfläche ist nur dann im Kopfbereich der Seite eingeblendet, wenn der Gültigkeitsbereich der **Übernehmen**-Schaltfläche auf *seitenübergreifend* gestellt ist - siehe „Verwaltung →Web Einstellungen“ auf Seite 54.

6.2 Menü Verwaltung

⌦ Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern - siehe „Benutzerauthentifizierung →Lokale Benutzer“ auf Seite 95. Solange dies noch nicht geschehen ist, erhalten Sie oben auf der Seite einen Hinweis darauf.

6.2.1 Verwaltung → Systemeinstellungen

Host



System (nur mGuard industrial)

Power supply 1 / 2
Zustand der beiden Netzteile.

Uptime
Bisherige Laufzeit des Geräts seit dem letzten Neustart.

Temperature (°C)
Wenn der hier angegebene Temperaturbereich unter- bzw. überschritten wird, dann wird ein SNMP-Trap ausgelöst.

System DNS Hostname

Hostnamen Modus
Mit *Hostnamen Modus* und *Hostname* können Sie dem mGuard einen Namen geben. Dieser wird dann z. B. beim Einloggen per SSH angezeigt (siehe „Verwaltung → Systemeinstellungen“, „Shell Zugang“ auf Seite 52) . Eine Namensgebung erleichtert die Administration mehrerer mGuards.

Nutzer definiert (siehe unten)
(Standard) Der im Feld **Hostname** eingetragene Name wird als Name für den mGuard gesetzt.

☞ Arbeitet der mGuard im *Stealth*-Modus, muss als *Hostnamen Modus* die Option *Nutzer definiert* gewählt werden.

Provider definiert (z. B. via DHCP)

Wenn der Netzwerkmodus ein externes Setzen des Hostnamens erlaubt wie z.B. bei DHCP, dann wird der vom Provider übermittelte Name für den mGuard gesetzt.

Hostname

Ist unter *Hostnamen Modus* die Option *Nutzer definiert* ausgewählt, dann tragen Sie hier den Namen ein, den der mGuard erhalten soll.

Sonst, d. h. wenn unter *Hostnamen Modus* die Option *Provider definiert (z. B. via DHCP)* ausgewählt ist, wird ein Eintrag in diesem Feld ignoriert.

Domain-Suchpfad

Erleichtert dem Benutzer die Eingabe eines Domain-Namens: Gibt der Benutzer den Domain-Name gekürzt ein, ergänzt der mGuard seine Eingabe um den angegebenen Domain-Suffix, der hier unter *Domain-Suchpfad* festgelegt wird.

SNMP Information

Systemname

Ein für Verwaltungszwecke frei vergebbarer Name für den mGuard, z. B. "Hermes", "Pluto". (Unter SNMP: sysName)

Standort

Frei vergebbare Bezeichnung des Installationsortes, z. B. "Maschinenraum", "Besenkammer". (Unter SNMP: sysLocation)

Kontakt

Angabe einer für den mGuard zuständigen Kontaktperson, am besten mit Telefonnummer. (unter SNMP: sysContact)

HiDiscovery

HiDiscovery ist ein Protokoll zur Unterstützung der initialen Inbetriebnahme von neuen Netzwerkgeräten und ist im Stealthmodus des mGuard aktiviert.

Lokale HiDiscovery Unterstützung

Aktiviert

Das HiDiscovery Protokoll ist aktiviert.

Nur lesend

Das HiDiscovery Protokoll ist aktiviert, der mGuard kann jedoch nicht darüber konfiguriert werden.

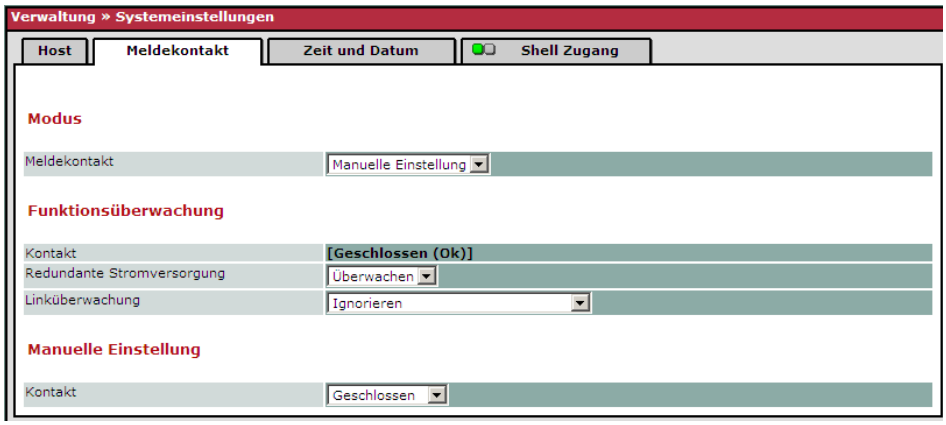
Deaktiviert

Das HiDiscovery Protokoll ist deaktiviert.

HiDiscovery Frame Durchleitung

Steht diese Option auf Ja, dann werden HiDiscovery Frames vom internen (LAN) Interface nach außen (WAN) weitergeleitet.

Meldekontakt (nur industrial)



Der Meldekontakt ist ein Relais, mit welchem der mGuard Fehlerzustände signalisieren kann. (Siehe auch „Meldekontakt“ auf Seite 24.)

Modus

Meldekontakt

Der Meldekontakt kann automatisch durch die **Funktionsüberwachung** geschaltet werden, oder durch **Manuelle Einstellung**.

Funktionsüberwachung

Kontakt

Zeigt den Zustand des Meldekontakts an. Entweder **Offen (Fehler)** oder **Geschlossen (Ok)**.

Redundante Stromversorgung

Bei **Ignorieren** hat der Zustand der Stromversorgung keinen Einfluß auf den Meldekontakt, bei **Überwachen** wird der Meldekontakt geöffnet bei Ausfall mindestens einer der zwei Versorgungsspannugen oder bei dauerhafter Störung im Guard (interne 3,3 VDC-Spannung, Versorgungsspannung < 9,6V, ...).

Linküberwachung

Überwachung des Linkstatus der Ethernetanschlüsse. Mögliche Einstellugen sind:

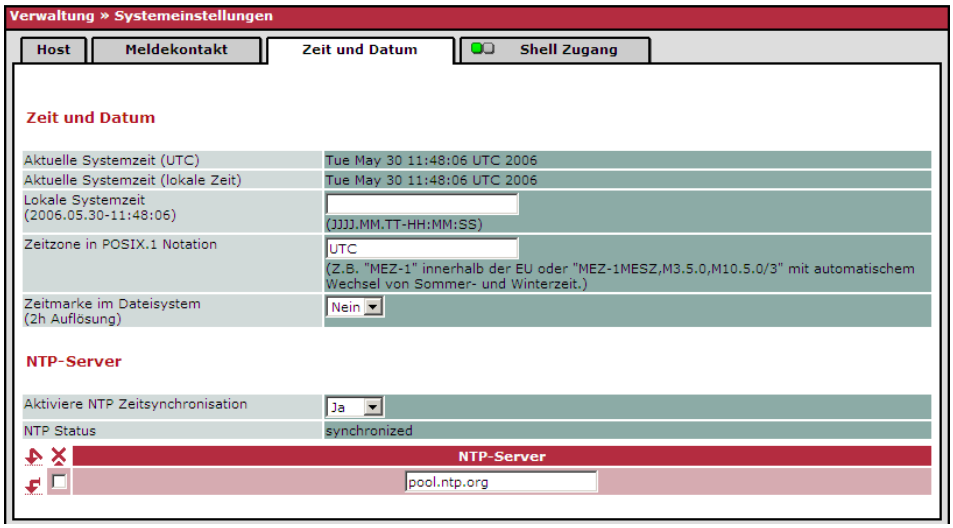
– Ignorieren
– Nur Intern (trusted) überwachen
– Nur Extern (untrusted) überwachen
– Beide überwachen

Manuelle Einstellung

Kontakt

Wenn für den Meldekontakt **Manuelle Einstellung** gewählt wurde, so kann man ihn hier auf **Geschlossen** oder **Offen (Alarm)** stellen.

Zeit und Datum



Zeit und Datum

Aktuelle Systemzeit (UTC)

Anzeige der aktuellen Systemzeit in Universal Time Coordinates (UTC). Solange die *NTP Zeitsynchronisation* noch nicht aktiviert ist (s. u.), und *Zeitmarken im Dateisystem* deaktiviert sind, beginnt die Uhr mit dem 1. Januar 2000.

Aktuelle Systemzeit (lokale Zeit)

Soll die eventuell abweichende aktuelle Ortszeit angezeigt werden, müssen Sie unter *Zeitzone in POSIX.1 Notation...* (s. u.) den entsprechenden Eintrag machen.

Lokale Systemzeit

Hier können Sie die Zeit des mGuards setzen falls kein NTP-Server eingestellt wurde (s. u.) oder aber der NTP-Server nicht erreichbar ist.

Das Datum und die Zeit werden in dem Format JJJJ.MM.TT-HH:MM:SS angegeben:

JJJJ	Jahr
MM	Monat
TT	Tag
HH	Stunde
MM	Minute
SS	Sekunde

Zeitzone in POSIX.1 Notation...

Soll oben unter *Aktuelle Systemzeit* nicht die mittlere Greenwich-Zeit angezeigt werden sondern Ihre aktuelle Ortszeit (abweichend von der mittleren Greenwich-Zeit), dann tragen Sie hier ein, um wieviel Stunden bei Ihnen die Zeit voraus bzw. zurück ist.

Beispiele:

In Berlin ist die Uhrzeit der mittleren Greenwich-Zeit um 1 Stunde voraus. Also tragen Sie ein: MEZ-1.

Wichtig ist allein die Angabe -1, -2 oder +1 usw., weil nur sie ausgewertet wird; die davor stehenden Buchstaben nicht. Sie können „MEZ“ oder beliebig anders lauten.

Wünschen Sie die Anzeige der MEZ-Uhrzeit (= gültig für Deutschland) mit automatischer Umschaltung auf Sommer- bzw. Winterzeit geben Sie ein: MEZ-1MESZ,M3.5.0,M10.5.0/3

Zeitmarke im Dateisystem (2h Auflösung): Ja / Nein

Ist dieser Schalter auf **Ja** gesetzt, schreibt der mGuard alle zwei Stunden die aktuelle Systemzeit in seinen Speicher.

Folge:

Wird der mGuard aus- und wieder eingeschaltet, wird nach dem Einschalten eine Uhrzeit in diesem 2-Stunden-Zeitfenster angezeigt und nicht eine Uhrzeit am 1. Januar 2000.

NTP-Server

Aktiviere NTP Zeitsynchronisation: Ja / Nein

Sobald das NTP aktiviert ist, bezieht der mGuard die Zeit aus dem Internet und zeigt diese als aktuelle Systemzeit an. Die Synchronisation kann einige Sekunden dauern.

Nur wenn dieser Schalter auf **Ja** steht und unter *NTP Server zur Synchronisation* (s. u.) mindestens ein Zeitserver angegeben ist, wird die aktuelle Systemzeit über das Internet bezogen.

NTP Status

Anzeige des aktuellen NTP-Status

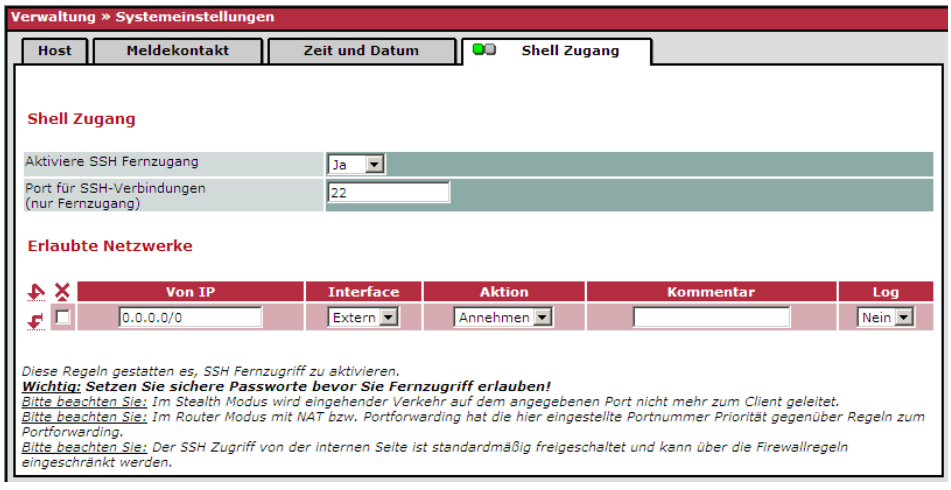
NTP-Server

Geben Sie hier einen oder mehrere Zeitserver an, von denen der mGuard die aktuelle Zeitangabe beziehen soll. Falls Sie mehrere Zeitserver angeben, verbindet sich der mGuard automatisch mit allen, um die aktuelle Zeit zu ermitteln.

☞ Wenn Sie statt einer IP-Adresse einen Hostnamen, z. B. pool.ntp.org, angeben, muss ein gültiger DNS-Server festgelegt sein - siehe „Netzwerk →DNS“ auf Seite 89.

☞ Arbeitet der mGuard im *Router- PPPoE-* oder *PPTP*-Modus, stellt er auch den angeschlossenen Rechnern die NTP-Zeit zur Verfügung.

Shell Zugang


Verwaltung » Systemeinstellungen
Host
Meldekontakt
Zeit und Datum
Shell Zugang
Shell Zugang
Aktiviere SSH Fernzugang
Ja
Port für SSH-Verbindungen (nur Fernzugang)
22
Erlaubte Netzwerke
Von IP
Interface
Aktion
Kommentar
Log
0.0.0.0/0
Extern
Annehmen
Nein
Diese Regeln gestatten es, SSH Fernzugriff zu aktivieren.
Wichtig: Setzen Sie sichere Passworte bevor Sie Fernzugriff erlauben!
Bitte beachten Sie: Im Stealth Modus wird eingehender Verkehr auf dem angegebenen Port nicht mehr zum Client geleitet.
Bitte beachten Sie: Im Router Modus mit NAT bzw. Portforwarding hat die hier eingestellte Portnummer Priorität gegenüber Regeln zum Portforwarding.
Bitte beachten Sie: Der SSH Zugriff von der internen Seite ist standardmäßig freigeschaltet und kann über die Firewallregeln eingeschränkt werden.

Shell Zugang

Bei eingeschaltetem SSH Fernzugang kann der mGuard von einem entfernten Rechner aus über die Kommandozeile konfiguriert werden.

Standardmäßig ist diese Option ausgeschaltet.

WICHTIG: Wenn Sie Fernzugriff ermöglichen, achten Sie darauf, dass ein sicheres Root- und Administrator-Passwort festgelegt ist.

Für SSH Fernzugang machen Sie folgende Einstellungen:

Aktiviere SSH Fernzugang: Ja / Nein

Wollen Sie SSH Fernzugriff ermöglichen, setzen Sie diesen Schalter auf **Ja**.

☞ Achten Sie in diesem Fall darauf, die auf dieser Seite befindlichen Firewall-Regeln unter **Erlaubte Netzwerke** so zu setzen, dass von außen auf den mGuard zugegriffen werden kann.

Port für SSH-Verbindungen (nur Fernzugang)

Standard: 22

Sie können einen anderen Port festlegen.

Die entfernte Gegenstelle, die den Fernzugriff ausübt, muss bei der Adressenangabe gegebenenfalls hinter der IP-Adresse die Port-Nummer angeben, die hier festgelegt ist.

Beispiel:

Ist dieser mGuard über die Adresse 123.456.789.21 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 22 festgelegt, dann muss bei der entfernten Gegenstelle im SSH-Client (z. B. PuTTY oder OpenSSH) diese Port-Nummer evtl. nicht angegeben werden.

Bei einer anderen Port-Nummer (z. B. 22222) ist diese anzugeben, z. B.:
ssh -p 22222 123.456.789.21

Erlaubte Netzwerke

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines SSH-Fernzugriffs.

Sie können (weitere) Regeln festlegen:

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugang erlaubt ist.

Bei den Angaben haben Sie folgende Möglichkeiten:

- IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140

Interface

Extern ODER **Intern**

Gibt an, ob die Regel für das externe oder interne Interface gelten soll.

Werksseitige Voreinstellung: Beim externen Interface wird alles verworfen, beim internen alles angenommen.

Aktion

Möglichkeiten:

- Annehmen
- Abweisen
- Verwerfen

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

☞ Im Stealth-Modus ist *Abweisen* als Aktion nicht möglich.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

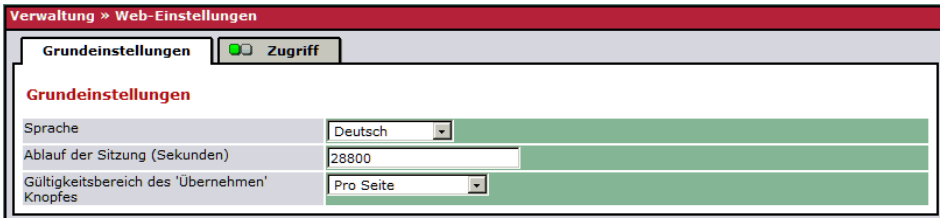
Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

6.2.2 Verwaltung →Web Einstellungen

Grundeinstellungen



Grundeinstellungen

Sprache

Ist in der Sprachauswahlliste **(Automatisch)** ausgewählt, übernimmt das Gerät die Spracheinstellung aus dem Browser des Rechners.

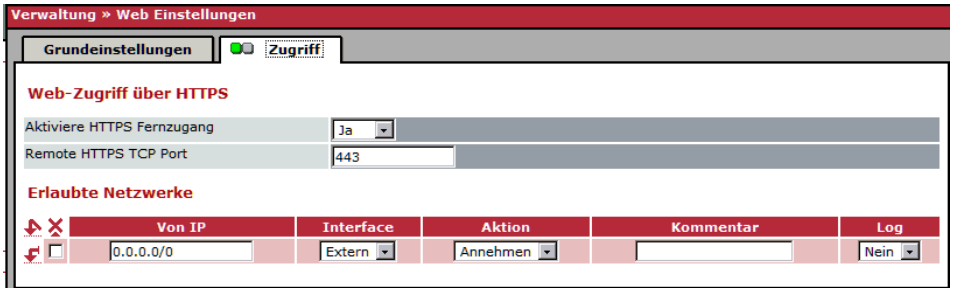
Ablauf der Sitzung (Sekunden)

Sekunden der Inaktivität, nach denen der Benutzer von der Web-Schnittstelle des mGuard automatisch abgemeldet wird. Mögliche Werte: 15 bis 86400 (= 24 Stunden)

Gültigkeitsbereich des 'Übernehmen' Knopfes

Legt fest, ob Sie nach Vornahme von Einstellungen auf mehreren Konfigurationsseiten für jede einzelne Seite **(Pro Seite)** die Schaltfläche **Übernehmen** zu klicken haben, oder ob Sie einmalig **Übernehmen** für Änderungen auf mehren Seiten **(Seitenübergreifend)** klicken müssen, damit die Einstellungen vom mGuad übernommen und in Kraft gesetzt werden.

Zugriff



Bei eingeschaltetem Web-Zugriff über HTTPS kann der mGuard über seine webbasierte Administratoroberfläche von einem entfernten Rechner aus konfiguriert werden. Das heißt, auf dem entfernten Rechner wird der Browser benutzt, um den lokalen mGuard zu konfigurieren.
Standardmäßig ist diese Option ausgeschaltet.

WICHTIG: Wenn Sie Fernzugriff ermöglichen, achten Sie darauf, dass ein sicheres Root- und Administrator-Passwort festgelegt ist.

Um HTTPS Fernzugang zu ermöglichen, machen Sie nachfolgende Einstellungen:

Web-Zugriff über HTTPS

Aktiviere HTTPS Fernzugang: Ja / Nein

Wollen Sie HTTPS Fernzugriff ermöglichen, setzen Sie diesen Schalter auf **Ja**.

☞ Achten Sie in diesem Fall darauf, die auf dieser Seite befindlichen Firewall-Regeln unter **Erlaubte Netzwerke** so zu setzen, dass von außen auf den mGuard zugegriffen werden kann.

Remote HTTPS TCP Port

Standard: 443

Sie können einen anderen Port festlegen.

Die entfernte Gegenstelle, die den Fernzugriff ausübt, muss bei der Adressenangabe hinter die IP-Adresse die Port-Nummer angeben, die hier festgelegt ist.

Beispiel:

Ist dieser mGuard über die Adresse 123.456.789.21 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 443 festgelegt, dann muss bei der entfernten Gegenstelle im Web-Browser diese Port-Nummer nicht hinter der Adresse angegeben werden.

Bei einer anderen Port-Nummer ist diese hinter der IP-Adresse anzugeben, z. B. wie folgt: https://123.456.7890.21:442/

Erlaubte Netzwerke

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines HTTP-Fernzugriffs.

Bei den Angaben haben Sie folgende Möglichkeiten:

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugang erlaubt ist.

Sie können (weitere) Regeln festlegen:

- IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140

Interface

Extern ODER **Intern**.

Gibt an, ob die Regel für das externe oder interne Interface gelten soll.

Werksseitige Voreinstellung: Beim externen Interface wird alles verworfen, beim internen alles angenommen.

Aktion

Möglichkeiten:

- Annehmen
- Abweisen

- Verwerfen

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen* - s. u.)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

☞ Im Stealth-Modus ist *Abweisen* als Aktion nicht möglich.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

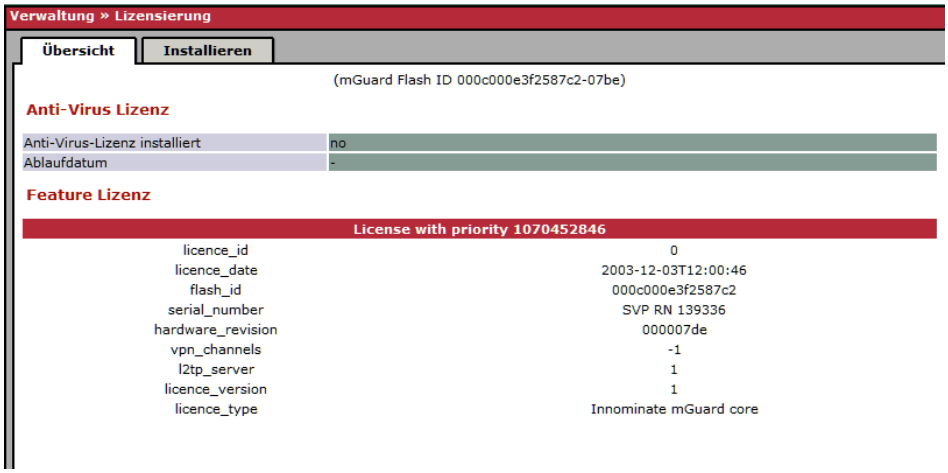
Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

6.2.3 Verwaltung →Lizensierung

Übersicht

Nur Anzeige



Anti-Virus Lizenz

Anti-Virus-Lizenz installiert

Zeigt an, ob eine Anti-Virus-Lizenz eingespielt ist.

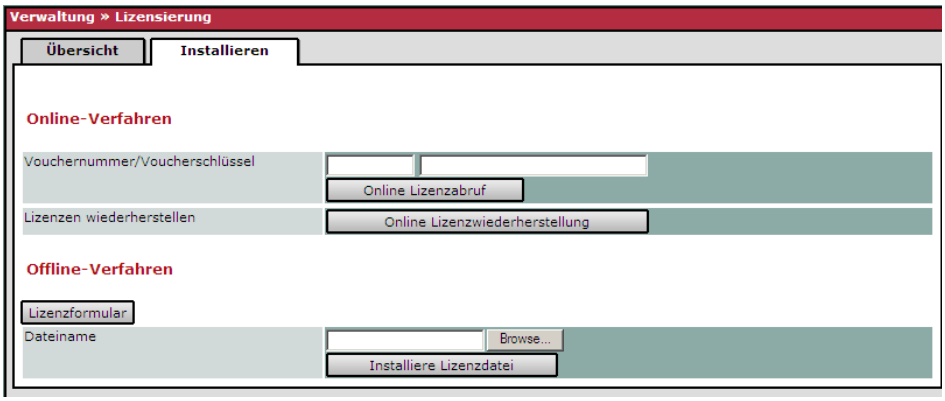
Ablaufdatum

Bei eingespielter Anti-Virus-Lizenz wird hier das Ablaufdatum dieser Lizenz angezeigt.

Feature Lizenz

Zeigt an, welche Funktionen die erworbene mGuard-Lizenz beinhaltet, z. B. die Anzahl der ermöglichten VPN-Tunnel, ob Remote Logging, ob MAU Management unterstützt werden usw.

Installieren



Sie können nachträglich Ihre erworbene mGuard-Lizenz um weitere Funktionen ergänzen. Auf diesem finden Sie einen Lizenz- bzw. Voucher-Key und eine Lizenz- bzw. Voucher-Seriennummer. Damit können Sie

1. die erforderliche Feature-Lizenzdatei anfordern und dann
2. die Lizenzdatei, die Sie daraufhin erhalten, installieren.

Online-Verfahren

Vouchernummer/Voucherschlüssel

Geben Sie hier die Seriennummer, die auf dem Voucher aufgedruckt ist, sowie den dazugehörigen Lizenz-Key ein und drücken Sie anschließend **Online Lizenzabruf**.

Der mGuard baut nun eine Verbindung über das Internet auf und installiert bei einem gültigen Voucher die zugehörige Lizenz auf dem mGuard.

Lizenzen wiederherstellen

Holt zuvor für diesen mGuard ausgestellte Lizenzen und installiert diese.

Offline-Verfahren

Nach Drücken der Schaltfläche **Lizenzformular** wird über eine Internet-Verbindung ein Formular bereit gestellt, über das Sie die gewünschte Lizenz bestellen können und in deren Felder Sie die folgenden Informationen eingeben:

Voucher Serial Number: Die Seriennummer, die auf Ihrem Vocher gedruckt ist

Voucher Key: Der Lizenz-Key auf Ihrem Voucher

Flash Id: Wird automatisch vorausgefüllt

Email Address: Ihre E-Mail-Adresse für die Zustellung der Lizenzdatei

Nach erfolgreichem Ausfüllen des Formulars wird Ihnen die Lizenzdatei zugesandt. Unter *Dateiname Lizenz* (s. u.) können Sie die Lizenzdatei einspielen.

Installiere Lizenz

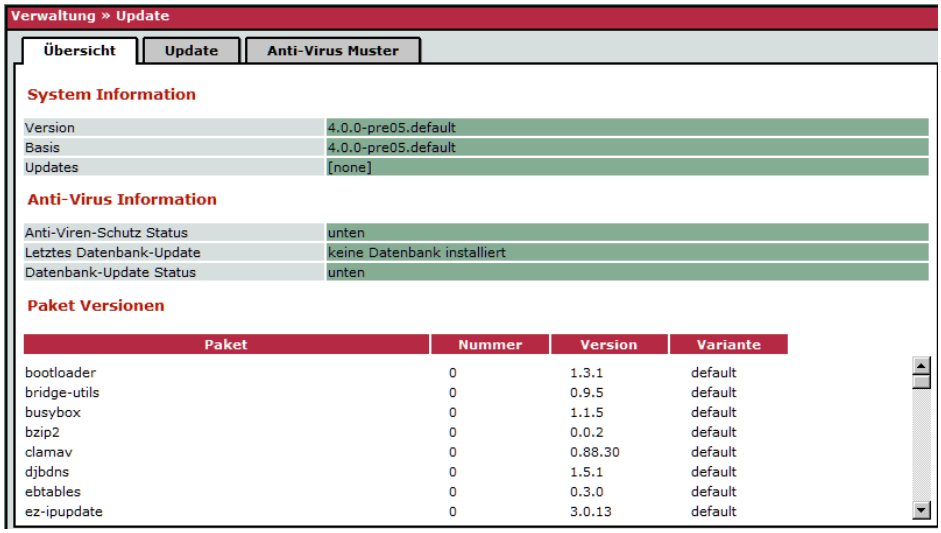
Nach Erwerb einer Lizenz wird die Lizenzdatei Ihnen als Anhang einer E-Mail zugesandt. Um die Lizenz einzuspielen, speichern Sie zunächst die Lizenz-Datei als separate Datei auf Ihrem Rechner und gehen dann wie folgt vor:

– Die Schaltfläche **Durchsuchen...** klicken, die Datei selektieren und öffnen, so dass ihr Pfad- bzw. Dateiname im Feld *Dateiname* angezeigt wird.
– Dann die Schaltfläche **Installiere Lizenzdatei** klicken.

6.2.4 Verwaltung →Update

Übersicht

Nur Anzeige



Sie können die erfolgreiche Freischaltung des Virenfilters überprüfen.
Die Information über das Ablaufdatum Ihrer Anti-Virus-Lizenz: Siehe „Verwaltung →Lizensierung“ auf Seite 56

System Information

Version
Die aktuelle Software-Version des mGuard

Basis
Die Software-Version, mit der dieser mGuard ursprünglich geflasht wurde.

Updates
Liste der Updates, die zur Basis hinzu installiert worden sind.

Anti-Virus Information

Antiviren-Schutz Status
Hier können Sie den Status der Scan-Engine überprüfen. Wenn die Überwachung für mindestens ein Protokoll aktiviert ist, wird hier der Status **up** angezeigt.

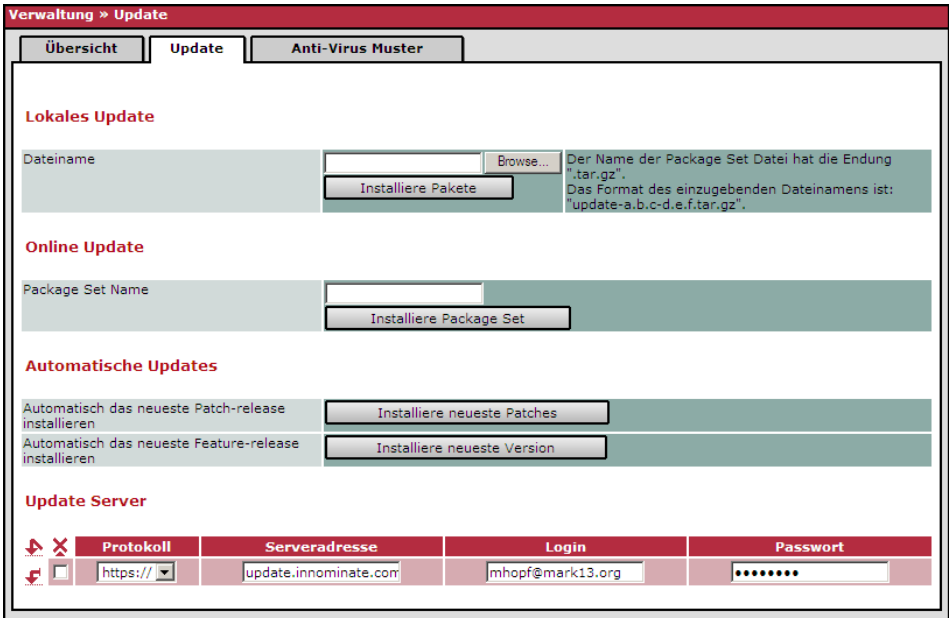
Letztes Datenbank-Update
Es werden die Versionsnummern und das Erstellungsdatum der Virensignaturen angezeigt.
Die Datenbank besteht aus den Dateien main.cvd und daily.cvd, wobei letztere häufiger aktualisiert wird.

Datenbank-Update Status
Hier wird angezeigt, ob die Datenbank-Aktualisierung aktiviert ist, ob gerade ein Datenbank-Update durchgeführt wird oder ob die Aktualisierung wegen einer abgelaufenen Antivirenlizenz gesperrt ist.

Paket Versionen

Listet die einzelnen Software-Module des mGuard auf. Gegebenenfalls für Supportzwecke interessant.

Update



Um ein Softwareupdate durchzuführen, gibt es zwei Möglichkeiten:

– Sie haben die aktuelle Package Set Datei auf Ihrem Rechner (der Dateiname hat die Endung ".tar.gz") und Sie führen ein lokales Update durch.

ODER

– Sie laden die Package Set Datei per Internet vom Update Server herunter und installieren dann die Pakete.

Lokales Update

Dateiname

Zur Installation von Paketen gehen Sie wie folgt vor:

1. Die Schaltfläche **Durchsuchen...** klicken, die Datei selektieren und öffnen, so dass ihr Pfad- bzw. Dateiname im Feld *Dateiname* angezeigt wird.
   Das Format des Dateinamens muss lauten: update-a.b.c-d.e.f.tar.gz
2. Dann die Schaltfläche **Installiere Pakete** klicken.

Online Update

Um ein Online Update duchzuführen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass unter **Update Server** mindestens ein gültiger Eintrag vorhanden ist. Die dafür nötigen Angaben haben Sie von Ihrem Lizenzgeber erhalten.
2. Geben Sie den Namen des Packagesets ein. z.B. "update-4.0.x-4.1.0".
3. Dann die Schaltfläche **Installiere Package Set** klicken.

Automatische Updates

Dieses ist eine Variante des Online Updates, bei welchem der mGuard den benötigten Package Set Namen eigenständig ermittelt.

Automatisch das neueste Patch-release installieren

Patch-releases beheben Fehler der vorherigen Versionen und haben eine Versionsnummer, welche sich nur in der dritten Stelle ändern.

Z.B. ist 4.0.1 ein Patch-release zur Version 4.0.0.

Automatisch das neueste Feature-release installieren

Feature-releases ergänzen den mGuard um neue Eigenschaften oder enthalten Änderungen am Verhalten des mGuard. Ihre Versionsnummer ändert sich in der ersten und zweiten Stelle.

Z.B. ist 4.1.0 ein Feature-release zu den Versionen 3.1.0 und 4.0.1.

Update Server

Legen Sie fest, von welchen Servern ein Update vorgenommen werden darf.

⌦ Die Liste der Server wird priorisiert von oben nach unten abgearbeitet, bis ein verfügbarer Server gefunden wird.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Der Update der kann entweder per HTTPS oder HTTP erfolgen.

Server Adresse

Hostnamen des Servers, der die Update-Dateien bereitstellt.

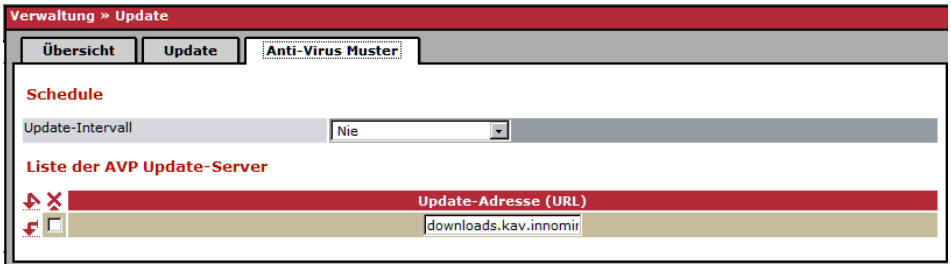
Login

Login für den Server. Beim Update mittels HTTP-Protokoll ist eine Angabe des Logins u.U. nicht erforderlich.

Passwort

Passwort für den Login. Beim Update mittels HTTP-Protokoll ist eine Angabe des Logins u.U. nicht erforderlich.

Anti-Virus Muster



Die Dateien mit den Virensignaturen (auch *Anti-Virus Pattern*, *Anti-Virus-Muster* oder *Virenerkennungs-Muster* genannt) können durch einen einstellbaren Update-Server in einem nutzerdefinierten Intervall aktualisiert werden. Das Update geschieht parallel zur Nutzung des Antivirenfilters. Im Auslieferungszustand befinden sich keine Virensignaturen auf dem mGuard. Deshalb sollte nach dem Aktivieren des Antiviren-Schutzes mit der entsprechenden Lizenz auch das Update-Intervall eingestellt werden. Der Verlauf des Updates kann im Antivirus-Update-Log verfolgt werden.

Schedule

Update-Intervall

Geben Sie hier an, ob - und wenn ja - in welchen Zeitabständen ein automatisches Update der Virenerkennungs-Muster stattfinden soll. Öffnen Sie dazu die Auswahlliste und wählen Sie den gewünschten Wert.

Die Gesamtgröße der Datenbank beträgt z.Zt. etwa 5 MByte. Die Datenbank ist aufgeteilt in zwei Dateien, von denen eine Datei mit einer Größe von maximal ca. 1MB häufig aktualisiert wird, während die andere Datei statisch ist

und wesentlich seltener aktualisiert wird. Es werden nur die auf dem Update-Server aktualisierten Dateien nachgeladen.

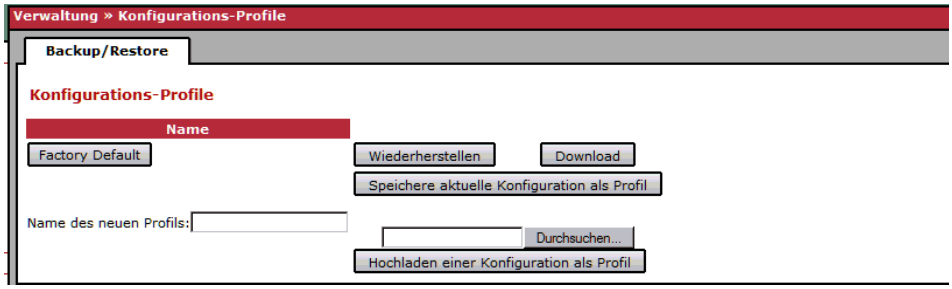
Liste der AVP Update-Server

Geben Sie hier den Namen von mindestes einem AVP Update-Server an.
Sie können die Server auswählen, von denen der Update der Virensignaturdatei geladen werden soll. Ein Standardserver ist bereits voreingetragen. Sie können bei Bedarf eigene Server angeben.

⌦ Die Liste der Server wird priorisiert von oben nach unten abgearbeitet, bis ein verfügbarer Server gefunden wird.

6.2.5 Verwaltung →Konfigurationsprofile

Backup / Restore



Sie haben die Möglichkeit, die Einstellungen des mGuard als Konfigurations-Profil unter einem beliebigen Namen im mGuard zu speichern. Sie können mehrere solcher Konfigurations-Profile anlegen, so dass Sie nach Bedarf zwischen verschiedenen Profilen wechseln können, z. B. wenn der mGuard in unterschiedlichen Umgebungen eingesetzt wird.
Darüber hinaus können Sie Konfigurations-Profile als Dateien auf ihrem Konfigurations-Rechners abspeichern. Umgekehrt besteht die Möglichkeit, eine so erzeugte Konfigurationsdatei in den mGuard zu laden und zu aktivieren.
Zusätzlich haben Sie die Möglichkeit, jederzeit die Werkseinstellung (= Factory Default) (wieder) in Kraft zu setzen.

⌦ Beim Abspeichern eines Konfigurations-Profils werden Passwörter nicht mitgespeichert.

Aktuelle Konfiguration als Konfigurations-Profil im mGuard speichern

1. In Feld *Name des neuen Profils* den gewünschten Namen eintragen
2. Die Schaltfläche **Speichere aktuelle Konfiguration als Profil** klicken.

Ein im mGuard gespeichertes Konfigurations-Profil anzeigen / aktivieren / löschen

Konfigurations-Profil anzeigen:
Den Namen des Konfigurations-Profils anklicken.

Konfigurations-Profil aktivieren:
Rechts neben dem Namen des betreffenden Konfigurations-Profils die Schaltfläche **Wiederherstellen** klicken.

Konfigurations-Profil löschen:
Rechts neben dem Namen des betreffenden Konfigurations-Profils die Schaltfläche **Löschen** klicken.
Das Profil **Factory Default** kann nicht gelöscht werden.

Konfigurations-Profil als Datei auf dem Konfigurationsrechner speichern

1. Rechts neben dem Namen des betreffenden Konfigurations-Profils die Schaltfläche **Download** klicken.
2. Legen Sie im angezeigten Dialogfeld den Dateinamen und Ordner fest, unter bzw. in dem das Konfigurations-Profil als Datei gespeichert wird.
   (Sie können die Datei beliebig benennen.)

Konfigurations-Profil vom Konfigurationsrechner auf den mGuard laden

Voraussetzung: Sie haben nach dem oben beschriebenem Verfahren ein Konfigurations-Profil als Datei auf dem Konfigurations-Rechners gespeichert.

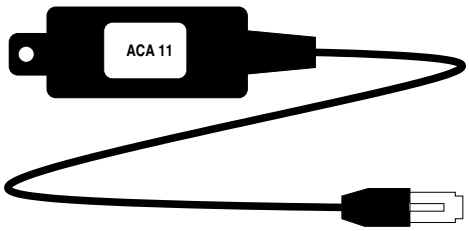
1. In Feld *Name des neuen Profils* den Namen eintragen, den das einzuladende Konfigurations-Profil erhalten soll.
2. Die Schaltfläche **Durchsuchen** klicken und dann die Datei selektieren.
3. Die Schaltfläche **Hochladen einer Konfiguration als Profil** klicken.
   Folge: Die hochgeladene Konfiguration erscheint in der Liste der Konfigurations-Profile.

Soll das hochgeladene Konfigurations-Profil aktiviert werden, klicken Sie neben dem Namen auf **Wiederherstellen.**

⌦ Wenn das Wiederherstellen einen Wechsel zwischen dem Stealth-Modus und einem der anderen Netzwerk-Modi beinhaltet, wird der mGuard neu gestartet.

Profile auf dem ACA11 (nur industrial)

Konfigurationsprofile können auch auf einem externen Autokonfurations-Adapter (ACA) abgelegt werden, der an die V.24 Buchse des mGuards angeschlossen werden kann.



Profil auf dem ACA11 speichern

- Wenn das Passwort auf dem mGuard, auf welchem das Profil später wieder eingelesen werden soll, ungleich "root" ist, dann muss dieses Passwort unter **Das root Passwort zur Speicherung auf dem ACA11** eingegeben werden.
- Drücken Sie die Schaltfläche **Speichere aktuelle Konfiguration auf dem ACA11**.

Die LEDs STATUS und V.24 blinken, bis das Speichern beendet ist.

Profil vom ACA11 laden

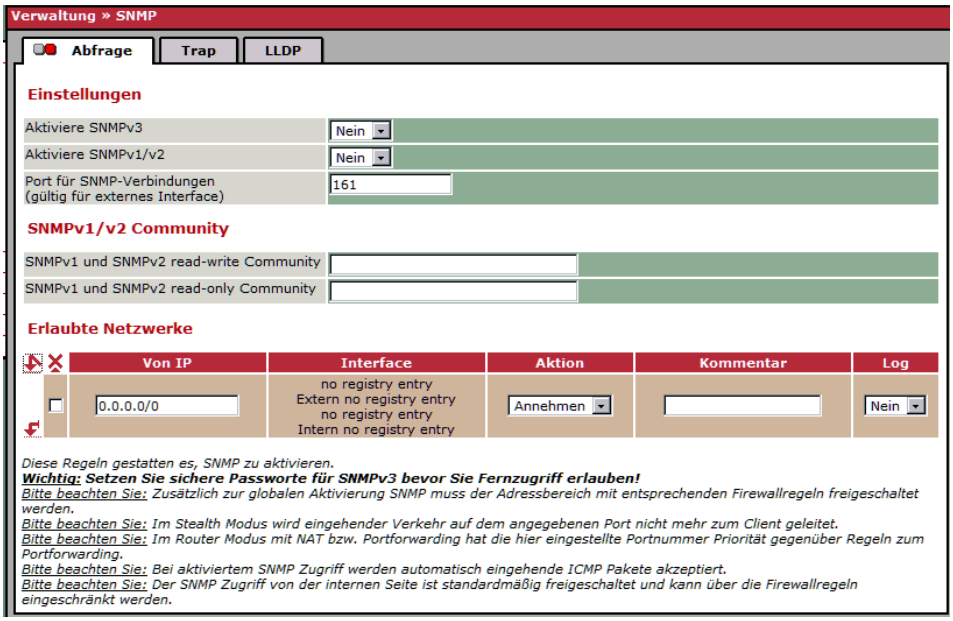
In die V.24 Buchse des mGuard den ACA11 einstecken. Bei eingestecktem ACA11 den mGuard starten. Das Passwort des mGuards muss entweder "root" lauten oder dem während des Speicherns des Profils angegebenen Passwort entsprechen.

Die LEDs STATUS und V.24 blinken, bis das Laden beendet ist.

⌦ Die Konfiguration auf dem ACA enthält auch die Passwörter für die Nutzer root, admin und user. Diese werden beim Laden vom ACA ebenfalls übernommen.

6.2.6 Verwaltung →SNMP (nur enterprise)

Abfrage


Verwaltung » SNMP
Abfrage
Trap
LLDP
Einstellungen
Aktiviere SNMPv3
Nein
Aktiviere SNMPv1/v2
Nein
Port für SNMP-Verbindungen (gültig für externes Interface)
161
SNMPv1/v2 Community
SNMPv1 und SNMPv2 read-write Community
SNMPv1 und SNMPv2 read-only Community
Erlaubte Netzwerke
Von IP
Interface
Aktion
Kommentar
Log
0.0.0.0/0
no registry entry
Extern no registry entry
no registry entry
Intern no registry entry
Annehmen
Nein
Diese Regeln gestatten es, SNMP zu aktivieren.
Wichtig: Setzen Sie sichere Passworte für SNMPv3 bevor Sie Fernzugriff erlauben!
Bitte beachten Sie: Zusätzlich zur globalen Aktivierung SNMP muss der Adressbereich mit entsprechenden Firewallregeln freigeschaltet werden.
Bitte beachten Sie: Im Stealth Modus wird eingehender Verkehr auf dem angegebenen Port nicht mehr zum Client geleitet.
Bitte beachten Sie: Im Router Modus mit NAT bzw. Portforwarding hat die hier eingestellte Portnummer Priorität gegenüber Regeln zum Portforwarding.
Bitte beachten Sie: Bei aktiviertem SNMP Zugriff werden automatisch eingehende ICMP Pakete akzeptiert.
Bitte beachten Sie: Der SNMP Zugriff von der internen Seite ist standardmäßig freigeschaltet und kann über die Firewallregeln eingeschränkt werden.

Das SNMP (Simple Network Management Protokoll) wird vorzugsweise in komplexeren Netzwerken benutzt, um den Zustand und den Betrieb von Geräten zu überwachen.

Das SNMP gibt es in mehreren Entwicklungsstufen: SNMPv1/SNMPv2 und SNMPv3.

Die älteren Versionen SNMPv1/SNMPv2 benutzen keine Verschlüsselung und gelten als nicht sicher. Daher ist davon abzuraten, SNMPv1/SNMPv2 zu benutzen.

SNMPv3 ist unter dem Sicherheitsaspekt deutlich besser, wird aber noch nicht von allen Management-Konsolen unterstützt.

⌦ SNMP-„Get“- oder „Walk“-Anfragen können länger als eine Sekunde dauern. Dieser Wert entspricht jedoch dem Standard-Timeout-Wert einiger SNMP-Management-Applikationen.
Bitte setzen Sie aus diesem Grund den Timeout-Wert Ihrer Management Applikation auf Werte zwischen 3 und 5 Sekunden, falls Timeout-Probleme auftreten sollten.

Einstellungen

Aktiviere SNMPv3: Ja / Nein

Wollen Sie zulassen, dass der mGuard per SNMPv3 überwacht werden kann, setzen Sie diesen Schalter auf **Ja**.

Für den Zugang per SNMPv3 ist eine Authentifizierung mittels Login und Passwort notwendig. Die Werkseinstellungen für die Login-Parameter lauten:

Login: admin

Passwort: SnmpAdmin

Für die Authentifizierung wird MD5 unterstützt, für die Verschlüsselung DES.

Die Login-Parameter für SNMPv3 können nur mittels SNMPv3 geändert werden.

Aktiviere SNMPv1/v2: Ja / Nein

Wollen Sie zulassen, dass der mGuard per SNMPv1/v2 überwacht werden kann, setzen Sie diesen Schalter auf **Ja**.

Zusätzlich müssen Sie unter **SNMPv1/v2 Community** die Login-Daten angeben.

Port für SNMP-Verbindungen (gültig für externes Interface)
Standard: 161

SNMPv1/v2 Community

SNMPv1 und SNMPv2 read-write Community

SNMPv1 und SNMPv2 read-only Community
Geben Sie in diese Felder die erforderlichen Login-Daten ein.

Erlaubte Netzwerke
Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines SNMP-Zugriffs.

Von IP
Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugang erlaubt ist.
Bei den Angaben haben Sie folgende Möglichkeiten:
- **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 140.

Interface
(fest vorgegeben).

Aktion
Möglichkeiten:
- Annehmen
- Abweisen
- Verwerfen

Annehmen bedeutet, die Datenpakete dürfen passieren.
Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.)
Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

☞ Im Stealth-Modus ist *Abweisen* als Aktion nicht möglich.

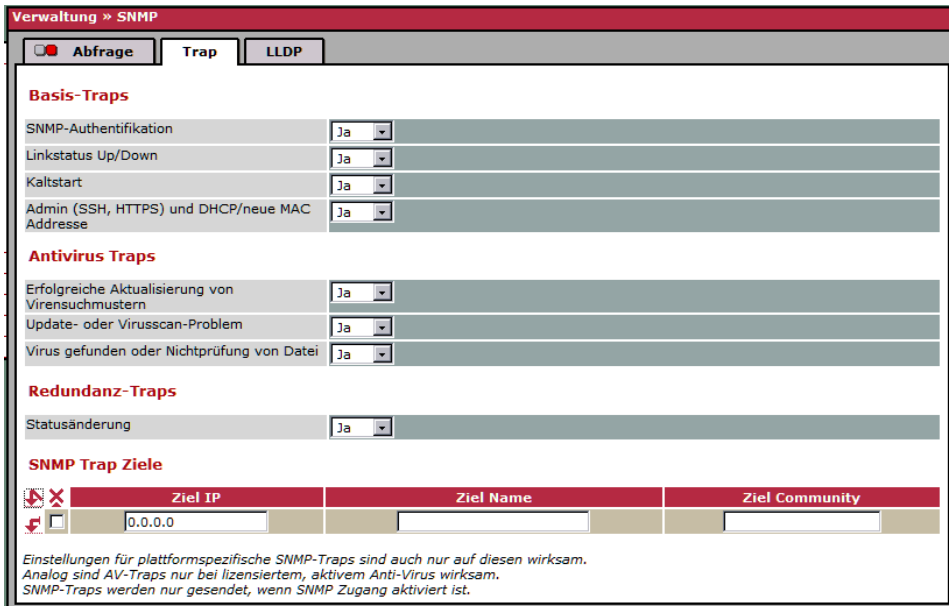
Kommentar
Ein frei wählbarer Kommentar für diese Regel.

Log
Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel
- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

⌦ Beachten Sie die unten auf der Webseite angegebenen Hinweise, hier noch einmal abgebildet::

Diese Regeln gestatten es, SNMP zu aktivieren.
***Wichtig:* Setzen Sie sichere Passworte für SNMPv3 bevor Sie Fernzugriff erlauben!**
Bitte beachten Sie: Zusätzlich zur globalen Aktivierung SNMP muss der Adressbereich mit entsprechenden Firewallregeln freigeschaltet werden.
Bitte beachten Sie: Im Stealth Modus wird eingehender Verkehr auf dem angegebenen Port nicht mehr zum Client geleitet.
Bitte beachten Sie: Im Router Modus mit NAT bzw. Portforwarding hat die hier eingestellte Portnummer Priorität gegenüber Regeln zum Portforwarding.
Bitte beachten Sie: Bei aktiviertem SNMP Zugriff werden automatisch eingehende ICMP Pakete akzeptiert.
Bitte beachten Sie: Der SNMP Zugriff von der internen Seite ist standardmäßig freigeschaltet und kann über die Firewallregeln eingeschränkt werden.

Trap



Bei bestimmten Ereignissen kann der mGuard SNMP Traps (→ Glossar) versenden. Die Traps entsprechen SNMPv1. Im folgenden sind die zu jeder Einstellung zugehörigenTrap-Informationen aufgelistet, deren genaue Beschreibung in der zum mGuard gehörenden MIB zu finden ist.

Basis-Traps

- **SNMP-Authentifikation**: Traps aktivieren **Ja / Nein**
  enterprise-oid : trapSenderIPenabledSystem
  generic-trap : authenticationFailure
  specific-trap : 0
- **Linkstatus Up/Down**: Traps aktivieren **Ja / Nein**
  enterprise-oid : trapSenderIPenabledSystem
  generic-trap : linkUp, linkDown
  specific-trap : 0
- **Kaltstart**: Traps aktivieren **Ja / Nein**
  enterprise-oid : trapSenderIPenabledSystem
  generic-trap : coldStart
  specific-trap : 0
- **Admin (SSH, HTTPS) Traps und neuer DHCP Client**: Traps aktivieren **Ja / Nein**
  enterprise-oid : mGuard
  generic-trap : enterpriseSpecific
  specific-trap : 1
  additional : hmSecHTTPSLastAccessIP

  enterprise-oid : mGuard
  generic-trap : enterpriseSpecific
  specific-trap : 2
  additional : hmSecShellSLastAccessIP

  enterprise-oid : mGuard
  generic-trap : enterpriseSpecific
  specific-trap : 3
  additional : hmSecHTTPSLastAccessMAC

Hardwarebezogene Traps (nur industrial)

- **Chassis (Stromversorgung, Relais)**: Traps aktivieren **Ja / Nein**

  enterprise-oid : mGuardTrapSenderIndustrial
  genericTrap : enterpriseSpecific
  specific-trap : 2
  additional : mGuardTrapIndustrialPowerStatus

  enterprise-oid : mGuardTrapSenderIndustrial
  genericTrap : enterpriseSpecific
  specific-trap : RelaisTrapSpecificNumber
  additional : mGuardTrapSignalRelaisState (mguardTrapSignlaRelaisTheReason, mGuardTrapSignal-RelaisReasonIndex)

- **Agent (ACA, Temperatur):** Traps aktivieren **Ja / Nein**

  enterprise-oid : trapSenderMguard
  genericTrap : enterpriseSpecific
  specific-trap : 1
  additional : mGuardSystemTemperature, mGuardTrapIndustrialTempHiLimit, mGuardTrapIndustrialLowLimit

  enterprise-oid : trapSenderMguard
  genericTrap : enterpriseSpecific
  specific-trap : 4
  additional : mGuardTrapAutoConfigAdapterChange

Blade Controller Traps (nur blade)

- **Statusänderung von Blades** (Umstecken, Ausfall): Traps aktivieren **Ja / Nein**

  enterprise-oid : mGuardBladeCTRL
  generic-trap : enterpriseSpecific
  specific-trap : 2
  additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlPowerStatus

  enterprise-oid : mGuardBladeCTRL
  generic-trap : enterpriseSpecific
  specific-trap : 3
  additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlRunStatus

- **Rekonfiguration von Blades** (Backup/Restore): Traps aktivieren **Ja / Nein**

  enterprise-oid : mGuardBladeCtrlCfg
  generic-trap : enterpriseSpecific
  specific-trap : 1
  additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlCfgBakkup

  enterprise-oid : mGuardBladeCtrlCfg
  generic-trap : enterpriseSpecific

specific-trap : 2
additional : mGuardTrapBladeRackID,
mGuardTrapBladeSlotNr,
mGuardTrapBladeCtrlCfgRestored

Antivirus SNMP-Traps

- **Erfolgreiche Aktualisierung von Virensuchmustern**: Traps aktivieren **Ja / Nein**

  enterprise-oid : mGuardTrapAv
  generic-trap : enterpriseSpecific
  specific-trap : 1
  additional : mGuardTResAvUpdateDone
- **Update- oder Virusscan-Problem**: Traps aktivieren **Ja / Nein**

  enterprise-oid : mGuardTrapAv
  generic-trap : enterpriseSpecific
  specific-trap : 2
  additional : mGuardTResAvUpdateError

  enterprise-oid : mGuardTrapAv
  generic-trap : enterpriseSpecific
  specific-trap : 5
  additional : mGuardTResAvFailed
- **Virus gefunden oder Nichtprüfung von Datei**: Traps aktivieren **Ja / Nein**

  enterprise-oid : mGuardTrapAv
  generic-trap : enterpriseSpecific
  specific-trap : 3
  additional : mGuardTResAvVirusDetected

  enterprise-oid : mGuardTrapAv
  generic-trap : enterpriseSpecific
  specific-trap : 4
  additional : mGuardTResAvFileNotScanned

Redundanz Traps

- **Statusänderung**: Traps aktivieren **Ja / Nein**.

  enterprise-oid : mGuardTrapRouterRedundancy
  genericTrap : enterpriseSpecific
  specific-trap : 1
  additional : mGuardTResRedundancyState,
  mGuardTResRedundancyReason

  enterprise-oid : mGuardTrapRouterRedundancy
  genericTrap : enterpriseSpecific
  specific-trap : 2
  additional : mGuardTResRedundancyBackupDown

SNMP Trap Ziele

Traps können an mehrere Ziele versendet werden.

Ziel IP

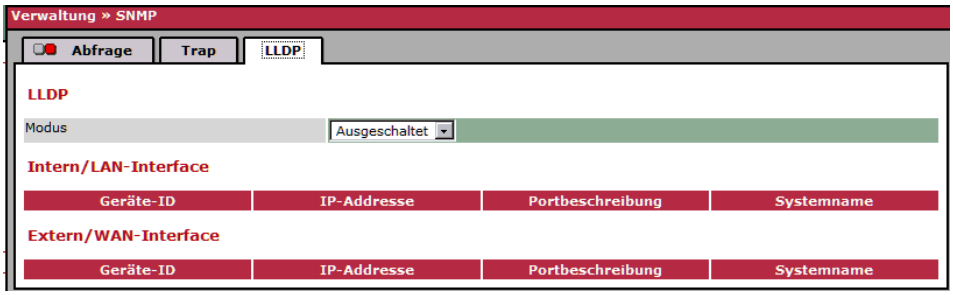
IP-Adresse, an welche der Trap gesendet werden soll.

Ziel Name

Ein optionaler beschreibender Name für das Ziel. Hat keinen Einfluss auf die generierten Traps.

Ziel Community
Name der SNMP-Community, welcher der Trap zugeordnet ist.

LLDP



Mit LLDP (Link Layer Discovery Protocol, IEEE 802.1AB/D13) kann mit geeigneten Abfragemethoden die (Ethernet) Netzwerk-Infrastruktur automatisch ermittelt werden. Auf Ethernet-Ebene (Layer 2) werden dazu periodisch Multicasts versandt. Aus deren Antworten werden dann Tabellen der ans Netz angeschlossenen Systeme erstellt, die über SNMP abgefragt werden können.

LLDP

Modus
Der LLDP-Service bzw. -Agent kann hier global ein- bzw. ausgeschaltet werden.

Intern/LAN-Interface
und

Extern/WAN-Interface

Geräte-ID
Eine eindeutige ID des gefundenen Rechners; üblicherweise eine seiner MAC-Adressen.

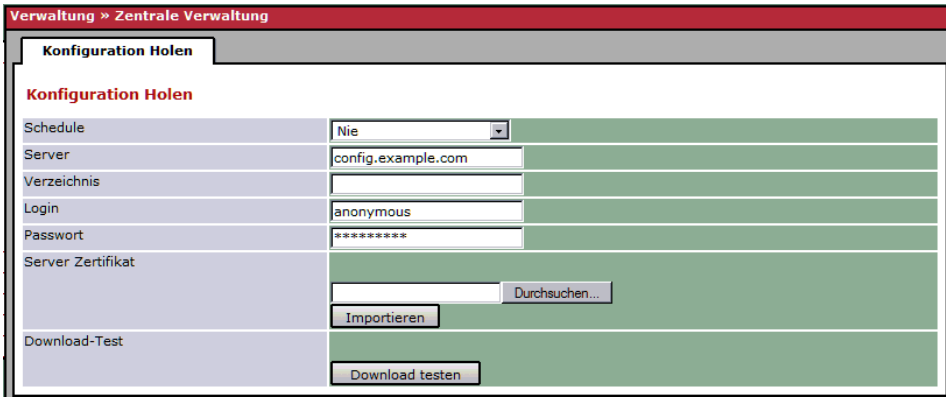
IP-Adresse
IP-Adresse des gefundenen Rechners über die der Rechner per SNMP administriert werden kann.

Portbeschreibung
Ein Text, welcher die Netzwerkschnittstelle beschreibt, über welche der Rechner gefunden wurde.

Systemname
Hostname des gefundenen Rechners.

6.2.7 Verwaltung →Zentrale Verwaltung

Konfiguration holen



Der mGuard kann sich in einstellbaren Zeitintervallen eine neue Konfiguration von einem HTTPS Server holen. Wenn sich die heruntergeladene Konfiguration von der aktuellen Konfiguration unterscheidet, wird die heruntergeladene Konfiguration automatisch aktiviert.

Konfiguration holen

Schedule
Geben Sie hier an, ob - und wenn ja - in welchen Zeitabständen eine neue Konfiguration vom Server heruntergeladen werden soll. Öffnen Sie dazu die Auswahlliste und wählen Sie den gewünschten Wert.

Server
IP-Adresse oder Hostname des Servers, welcher die Konfigurationen bereitstellt.

Verzeichnis
Das Verzeichnis (Ordner) auf dem Server, in dem die Konfiguration liegt.

Login
Login (Benutzername), das/den der HTTPS Server abfragt.

Passwort
Passwort, das der HTTPS Server abfragt.

Server Zertifikat
Das Zertifikat, das den HTTPS Server beglaubig, von dem die Konfiguration geholt wird. Das Zertifikat verhindert, dass nicht authorisierte Konfigurationen auf dem mGuard installiert werden.

☞ Der Name der Konfigurationsdatei auf dem HTTPS Server ist die Seriennummer des mGuards inklusive der Endung „.atv“.

☞ Wenn die hinterlegten Konfigurationsprofile auch den privaten VPN-Schlüssel für die VPN-Verbindung oder VPN-Verbindungen mit PSK enthalten, sollten folgende Bedingungen erfüllt sein:

- Das Passwort sollte aus mindestens 30 zufälligen Groß- und Kleinbuchstaben sowie Ziffern bestehen, um unerlaubten Zugriff zu verhindern.
- Der HTTPS Server sollte über den angegebenen Login nebst Passwort nur Zugriff auf die Konfiguration dieses einen mGuard ermöglichen. Ansonsten könnten sich die Nutzer anderer mGuards Zugriff verschaffen.

☞ Selbstunterschriebene Zertifikate (self-signed) sollten nicht die „key-

usage“ Erweiterung verwenden.

Download-Test

Durch Klicken auf die Schaltfläche Download-Test können Sie - ohne zuvor die angegebenen Parameter gespeichert zu haben - testen, ob die angegebenen Parameter funktionieren. Das Ergebnis des Tests wird rechts angezeigt; es wird keine Konfigurationsdatei heruntergeladen und in Kraft gesetzt.

⌧ Stellen Sie sicher, dass das Profil auf dem Server keine unerwünschten mit „GAI_PULL_“ beginnenden Variablen enthält, welche die hier vorgenommene Konfiguration überschreiben.

6.2.8 Verwaltung →Redundanz (nur enterprise XL)

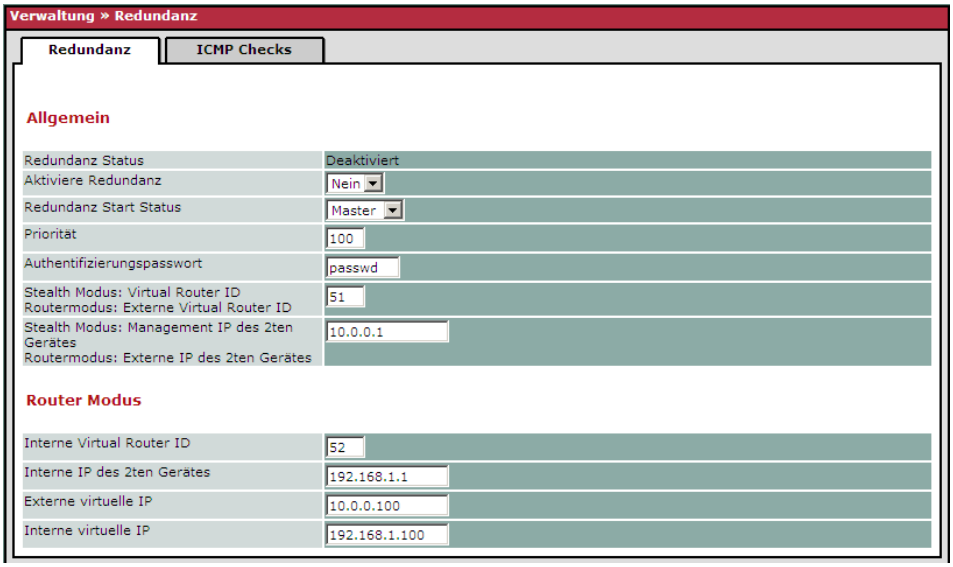
Mit Hilfe der Redunzanzfähigkeit ist es möglich, zwei mGuards zu einem einzigen virtuellen Router zusammenzufassen. Dabei übernimmt der zweite mGuard (Backup) in einem Fehlerfall die Funktion des ersten mGuards (Master).
Dazu wird der Zustand der Statefull Firewall zwischen beiden mGuards fortwährend synchronisiert, so dass bei einem Wechsel bestehende Verbindungen nicht abgebrochen werden.

⌧ Voraussetzung: Beide mGuards müssen entsprechend konfiguriert werden. Die Firewalleinstellungen sollten identisch sein, damit nach der Umschaltung keine Probleme auftreten.
⌧ Redundanz wird in folgenden Netzwerk-Modi unterstützt: *Router-Modus, Stealth Modus statisch* mit Management IP und im *Stealth Modus (mehrere Clients)*.
⌧ Bei aktivierter Redundanz dürfen die beiden mGuards nicht als VPN-Gateway genutzt werden.
⌧ Bei Geräten, die mit dem internen Netzwerk der mGuards verbunden sind, muss die interne virtuelle IP-Adresse als Standardgateway konfiguriert werden.

Die folgenden Funktionen können bei aktivierter Redundanz genutzt werden - siehe „Menü Netzwerksicherheit (nicht blade Controller)“:

- Eingehende/ausgehende Firewall Regeln
- NAT (IP-Masquerading, d. h. ausgehender Netzwerkverkehr wird auf die externe virtuelle IP umgeschrieben.)
- 1:1 NAT
- Port Weiterleitung (für *Eingehend auf IP* muß die externe virtuelle IP konfiguriert werden)
- MAC-Filter

Redundanz



State

Redundanz Status
Zeigt den aktuellen Status an.

Aktiviere Redundanz: Ja/ Nein
Redundanz aktivieren/deaktivieren.

Redundanz Start Status
Status des mGuards bei Aktivierung der Redundanz (*Master* oder *Backup*).

Priorität
Entscheidet, welcher mGuard als Master fungiert.
Sind die Prioriäten unterschiedlich gesetzt, so arbeitet der mGuard mit der höheren Priorität als Master, solange er nicht ausfällt.
Haben beide mGuards die gleiche Priorität und wird im Fehlerfall der Backup zum Master, so arbeitet dieser auch dann als Master weiter, wenn der vorherige mGuard wieder zur Verfügung steht.
Werte zwischen 1 und 254 sind möglich.

Authentifizierungspasswort
Das Passwort soll vor Fehlkonfigurationen schützen, bei denen sich mehrere virtuelle Router gegenseitig stören.
Das Passwort muss auf beiden mGuards gleich sein. Es wird im Klartext übermittelt und sollte daher nicht identisch mit anderen sicherheitsrelevanten Passwörtern sein.

Stealthmodus: Virtual Router ID
Routermodus: Externe Virtual Router ID
Eine ID zwischen 1 und 255, die auf beiden mGuards gleich sein muss und den virtuellen Router identifiziert.

Stealthmodus: Management IP des 2ten Gerätes
Routermodus: Externe IP des 2ten Gerätes
Im Stealthmodus die Management IP des zweiten mGuards, im Routermodus die externe IP-Adresse des zweiten mGuards.

Router Modus

Die folgenden Werte müssen gesetzt werden, wenn die mGuards im Router Mo-

dus betrieben werden.

Interne Virtual Router ID

Eine ID zwischen 1 und 255, die auf beiden mGuards gleich sein muss. Diese ID identifiziert den virtuellen Router am internen Interface.

Interne IP des 2ten Gerätes

Die interne IP-Adresse des zweiten mGuards. Die interne IP-Adresse ist die, unter der der mGuard vom lokal direkt angeschlossenen Client erreichbar ist.

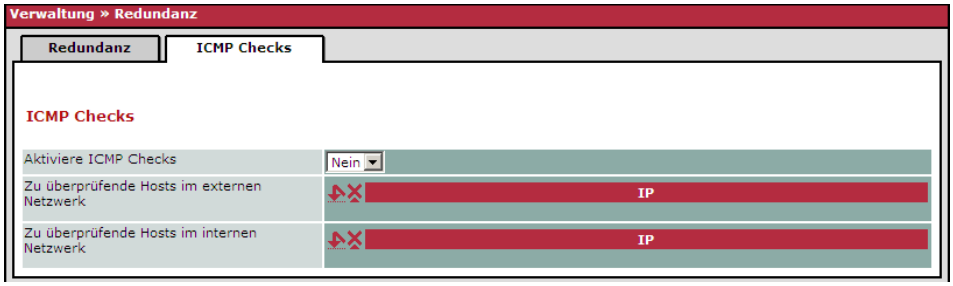
Externe virtuelle IP

Virtuelle IP-Adresse, über die der Verkehr durch den mGuard läuft. Wird z. B. bei NAT als externe IP verwendet.

Interne virtuelle IP

Virtuelle IP-Adresse, über die der Verkehr durch den mGuard läuft. Muss z. B. bei den Clients im internen Netzwerk als Default-Gateway eingestellt werden.

ICMP Checks



ICMP Checks bilden eine zusätzliche Möglichkeit der Überwachung der Netzwerkverbindungen zwischen den mGuards, die als virtueller Router zusammenarbeiten.

Fällt nur die interne oder die externe Netzwerkverbindung zwischen Master und Backup aus, so wird der Backup zum Master. Das vom Guard verwendete Virtual Router Redundancy Protocol (VRRP) kann den noch funktionierenden Master jedoch nicht darüber informieren. Über die noch funktionierenden Netzwerkverbindung würden die zwei Master anschließend miteinander in Konflikt stehen.

Über die ICMP Checks (ICMP Ping) kann der Master daher die Verbindung zum Backup überprüfen und sich gegebenenfalls deaktivieren.

Aktiviere ICMP Checks: Ja / Nein

Bei **Ja** wird die Verbindung zum Backup mit Hilfe des ICMP Protokolls überwacht.

Ist der Backup mGuard nicht mehr zu erreichen, versucht der Master nacheinander die Hosts zu erreichen, die unter *Zu überprüfende Hosts im externen/ internen Netzwerk* angegebenen sind.

Sind auch diese nicht erreichbar, deaktiviert sich der Master.

Zu überprüfende Hosts im externen Netzwerk

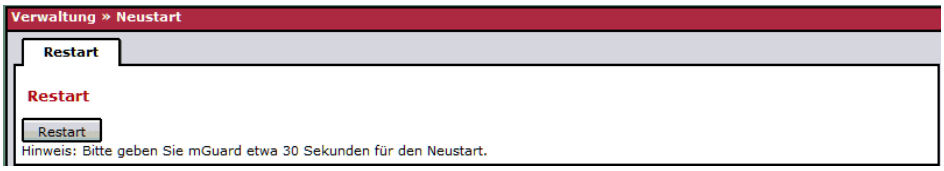
Zu überprüfende Hosts im internen Netzwerk

Geben Sie jeweils die IP-Adresse an.

Hosts müssen ICMP Echo Requests beantworten können.

6.2.9 Verwaltung →Neustart

Restart

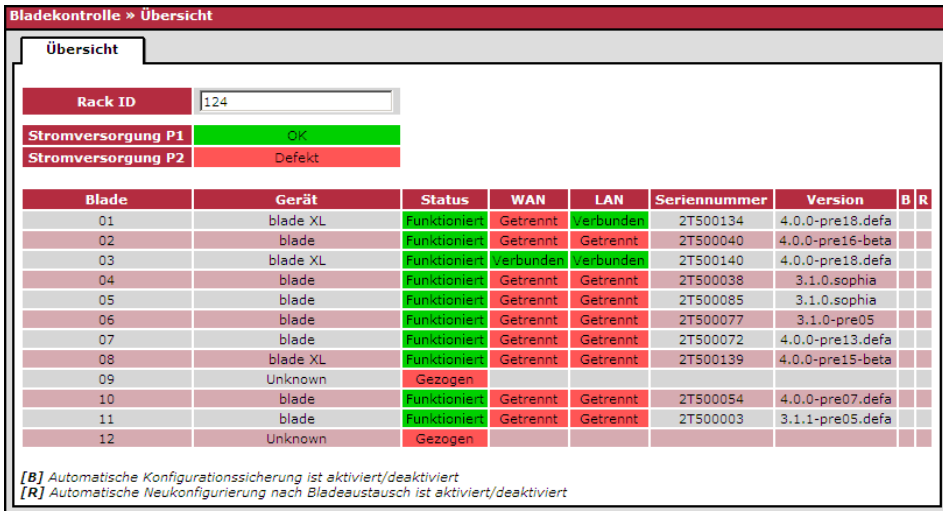


Startet den mGuard neu. Hat den selben Effekt, als wenn Sie die Stromzufuhr vorübergehend unterbrechen, so dass der mGuard aus- und wieder eingeschaltet wird.
Ein Neustart (= Reboot) ist erforderlich im Fehlerfall. Außerdem kann es erforderlich sein nach einem Software-Update.

6.3 Menü Bladekontrolle (nur blade Controller)

Dieses Menü steht nur auf dem Kontroller Blade zur Verfügung.

6.3.1 Bladekontrolle → Übersicht



Rack ID

Die ID des Racks, in dem sich der mGuard befindet. Auf dem Controller kann dieser Wert für alle blades konfiguriert werden.

Stromversorgung P1/P2

Status der Netzteile P1 und P2.

- OK
- Gezogen
- Defekt
- Fataler Fehler

Blade

Nummer des Slots, in welchem das mGuard blade steckt.

Gerät

Name des Geräts, z.B. „blade“ oder „blade XL“.

Status

Funktioniert - Das Gerät in dem Slot ist funktionsbereit.

Gesteckt - Das Gerät ist vorhanden, aber noch nicht bereit, z. B. weil es gerade beim Starten ist.

Gezogen - In dem Slot wurde kein Gerät entdeckt.

WAN

Status des Ethernet WAN Anschlusses.

LAN

Status des Ethernet LAN Anschlusses.

Seriennummer

Seriennummer des mGuards.

Version

Softwareversion des mGuards.

B

Backup: Für diesen Slot ist die automatische Konfigurationssicherung auf dem Controller aktiviert/deaktiviert.

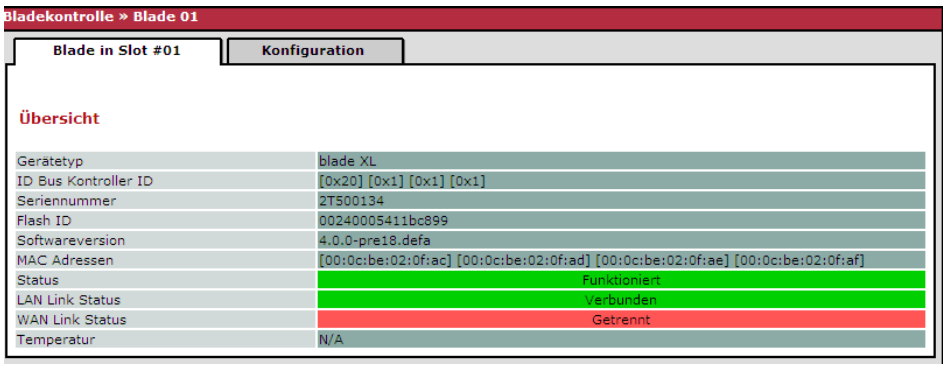
R

Restore: Für diesen Slot ist das automatische Zurückspielen der Konfiguration nach Austausch des mGuards aktiviert/deaktiviert.

6.3.2 Bladekontrolle → Blade 01 bis 12

Diese Seiten zeigen für jeden installierten mGuard Statusinformationen an und erlauben das Speichern und Zurückspielen der Konfiguration des jeweiligen mGuards.

Blade in slot #__



Gerätetyp

Name des Geräts, z.B. „blade“ oder „blade XL“.

ID bus Controller ID

ID dieses Slots am Controllbus der bladeBase.

Seriennummer

Seriennummer des mGuards.

Flash ID

Flash ID des Flashspeichers des mGuards.

Software Version

Die Version der auf dem mGuard installierten Software.

MAC adressen

Alle vom mGuard verwendeten MAC-Adressen.

Status

Status des mGuards.

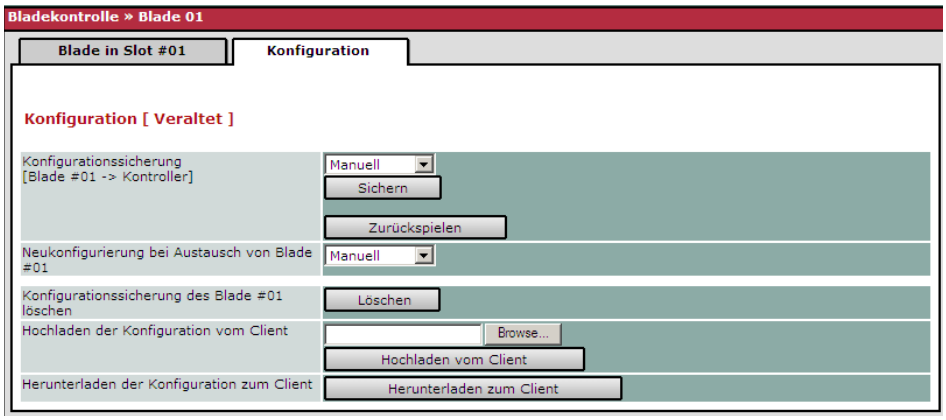
LAN Status

Status des Ethernet LAN Anschlusses.

WAN Status

Status des Ethernet WAN Anschlusses.

Konfiguration



Konfigurationssicherung [Blade #__ -> Kontroller]

Automatisch: Kurz nach einer Konfigurationsänderung des mGuards wird die neue Konfiguration automatisch auf dem Controller gespeichert.

Manuell: Die Konfiguration kann mit **Sichern** auf dem Controller gesichert und mit **Zurückspielen** wieder auf den mGuard zurückgespielt werden.

Neukonfiguration bei Austausch des Blade

Beim Austausch eines mGuards in diesem Slot wird die auf dem Controller gespeicherte Konfiguration auf das neue Gerät in diesem Slot übertragen.

Konfigurationssicherung des Blade #__ löschen

Löscht die auf dem Controller gespeicherte Konfiguration für das Gerät in diesem Slot.

Hochladen der Konfiguration vom Client

Speichert das angegebene Konfigurationsprofil des Gerätes in diesem Slot auf dem Controller.

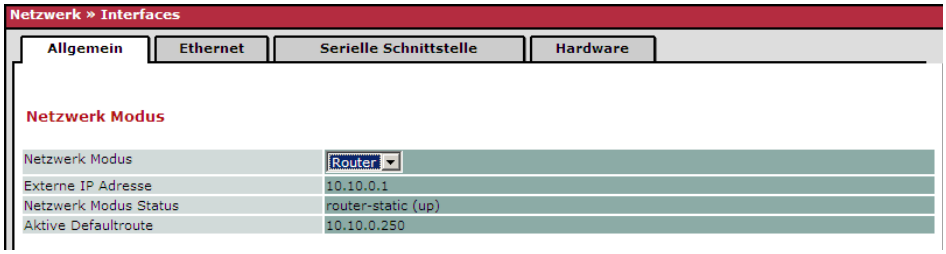
Herunterladen der Konfiguration zum Client

Lädt das auf dem Controller gespeicherte Konfigurationsprofil herunter ins Gerät.

6.4 Menü Netzwerk

6.4.1 Netzwerk →Interfaces

Allgemein



Netzwerk Modus

Der mGuard muss auf den Netzwerk-Modus (= Betriebsart) gestellt werden, der seiner lokalen Rechner- bzw. Netzwerk-Anbindung entspricht. Siehe „Typische Anwendungsszenarien“ auf Seite 10

.

Je nach dem, auf welchen Netzwerk-Modus der mGuard gestellt ist, ändert sich auch die Seite mit den auf ihr angebotenen Konfigurationsparametern

- **Stealth** *(Werkseinstellung außer mGuard delta*)
  Der *Stealth*-Modus wird verwendet, um einen einzelnen Computer oder ein Netzwerk an den mGuard anzuschließen. Wesentlich ist Folgendes: Ist der mGuard im Netzerk-Modus (= Betriebsart) *Stealth*, muss beim angeschlossenen Client (Einzelrechner oder Netzwerk) keine Neukonfiguration der Schnittstelle zum mGuard vorgenommen werden.
  Im *Stealth*-Modus kann der mGuard einfach in eine bestehende Netzwerkanbindung des betreffenden Rechners oder Netzes integriert werden. Dazu wird er einfach zwischengeschaltet.
  Der mGuard analysiert den laufenden Netzwerkverkehr und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig und arbeitet transparent, d. h. ohne dass der Client umkonfiguriert werden muss.
  Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall und VPN zur Verfügung.
  Von extern gelieferte DHCP-Daten werden an den angeschlossenen Client durchgelassen.
  - ☞ Eine auf dem Client installierte Firewall muß ICMP Echo Requests (Ping) zulassen, wenn der mGuard Dienste wie VPN, DNS, NTP, etc. bereit stellen soll.
  - ☞ Im *Stealth* Modus hat der mGuard folgende interne Adresse: 1.1.1.1
  - ☞ Über sein internes Interface ist der mGuard an ein lokales Netzwerk oder an ein Einzelrechner angeschlossen.
    Damit der mGuard für Konfigurationszwecke über die IP-Adresse 1.1.1.1 vom Client erreichbar ist, muss das auf dem Client konfigurierte Standardgateway erreichbar sein.

- **Router** *(Werkseinstellung mGuard delta)*
  Befindet sich der mGuard im *Router*-Modus, arbeitet er als Gateway zwischen verschiedenen Teilnetzen und hat dabei ein externes und ein internes Interface mit jeweils mindestens einer IP-Adresse.
  Externes Interface:

Über sein externes Interface (WAN) ist der mGuard ans Internet oder an weitere Teile des LAN angeschlossen.

- mGuard smart: die Ethernetbuchse

Internes Interface:

Über sein internes Interface (LAN) ist der mGuard an ein lokales Netzwerk oder an ein Einzelrechner angeschlossen:

- mGuard smart: der Ethernetstecker
- mGuard PCI: Im *Treibermodus* ist dies die Netzwerk-Schnittstelle des Betriebssystems zum angeschlossenen Netzwerk oder im *Power-over-PCI Modus* die LAN Buchse.

Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall und VPN zur Verfügung.

☞ Wird der mGuard im *Router*-Modus betrieben, muss er bei lokal angeschlossenen Client-Rechnern als Standardgateway festgelegt sein. D. h. bei diesen Rechnern ist die interne IP-Adresse des mGuard als Adresse des Standardgateway anzugeben. Siehe „IP-Konfiguration bei Windows-Clients“ auf Seite 94.

☞ Wird der mGuard im *Router*-Modus betrieben und stellt die Verbindung zum Internet her, sollte NAT aktiviert werden. Nur dann erhalten die Rechner im angeschlossenen lokalen Netz über den mGuard Zugriff auf das Internet - siehe „Netzwerksicherheit → NAT“ auf Seite 103. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.

- **PPPoE**

  Der *PPPoE*-Modus entspricht dem Router-Modus mit DHCP - mit einem Unterschied: Für den Anschluss ans externe Netzwerk (Internet, WAN) wird - wie in Deutschland - das PPPoE-Protokoll verwendet, das von vielen DSL-Modems (bei DSL-Internetzugang) verwendet wird. Die externe IP-Adresse, unter der der mGuard von einer entfernten Gegenstelle aus erreichbar ist, wird vom Provider festgelegt.

  ☞ Wird der mGuard im *PPPoE*-Modus betrieben, muss bei lokal angeschlossenen Client-Rechnern der mGuard als Default-Gateway festgelegt sein. D. h. bei diesen Rechnern ist die interne IP-Adresse des mGuard als Adresse des Standardgateway anzugeben. Siehe „IP-Konfiguration bei Windows-Clients“ auf Seite 94.

  ☞ Arbeitet der mGuard im *PPPoE*-Modus, muss NAT aktiviert werden, um Zugriff auf das Internet zu erhalten - siehe „Netzwerksicherheit → NAT“ auf Seite 103. Ist NAT nicht aktiviert, können eventuell nur VPN-Verbindungen genutzt werden.

- **PPTP**

  Ähnlich dem *PPPoE*-Modus. In Österreich zum Beispiel wird statt des PPPoE-Protokolls das PPTP-Protokoll zur DSL-Anbindung verwendet.
  (PPTP ist das Protokoll, das ursprünglich von Microsoft für VPN-Verbindungen benutzt worden ist.)

  ☞ Wird der mGuard im *PPTP*-Modus betrieben, muss bei lokal angeschlossenen Client-Rechnern der mGuard als Standardgateway festgelegt sein. D. h. bei diesen Rechnern ist die interne IP-Adresse des mGuard als Adresse des Standardgateway anzugeben. Siehe „IP-Konfiguration bei Windows-Clients“ auf Seite 94.

  ☞ Wird der mGuard im *PPTP*-Modus betrieben, sollte NAT aktiviert wer-

den, um aus dem lokalen Netz heraus Zugriff auf das Internet zu erhalten - siehe „Netzwerksicherheit → NAT“ auf Seite 103. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.

- Beim Wechsel des Netzwerk-Modus in oder aus dem *Stealth*-Modus bootet das Gerät automatisch neu.
- Wenn Sie die Adresse des mGuard ändern (z. B. durch Wechsel des Netzwerk-Modus von *Stealth* auf *Router*), dann ist das Gerät nur noch unter der neuen Adresse zu erreichen. Erfolgte die Änderung über das lokale Interface, so erhalten Sie eine Rückmeldung über die neue Adresse, bevor die Änderung aktiv wird. Bei Änderungen vom externen Interface aus erhalten Sie keine Rückmeldungen.
- Wenn Sie den Modus auf *Router* oder *PPPoE* oder *PPTP* stellen und dann die interne IP-Adresse und/oder die lokale Netzmaske ändern, achten Sie unbedingt darauf, dass Sie korrekte Werte angeben. Sonst ist der mGuard nicht mehr erreichbar.

Externe IP Adresse

Die Adressen, unter denen der mGuard von Geräten des externen Netzes aus erreichbar ist. Sie bilden die Schnittstelle zu anderen Teilen des LAN oder zum Internet. Findet hier der Übergang zum Internet statt, werden die IP-Adressen vom Internet Service Provider (ISP) vorgegeben.Wird dem mGuard eine IP-Adresse dynamisch zugeteilt, können Sie hier die gerade gültige IP-Adresse nachschlagen.

Im *Stealth*-Modus übernimmt der mGuard die Adresse des lokal angeschlossenen Rechners als seine externe IP.

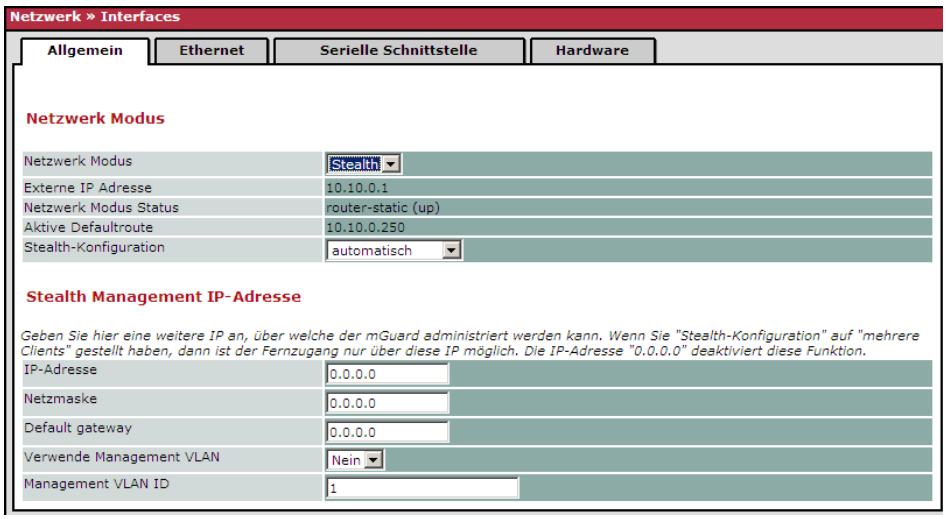
Netzwerk Modus Status

Anzeige des Status des ausgewählten Netzwerk Modus.

Aktive Defaultroute

Hier wird die IP-Adresse angezeigt, über die der mGuard versucht, ihm unbekannte Netze zu erreichen. Hier steht „(none)“, wenn sich der mGuard im *Stealth*-Modus befindet, oder falls die IP-Adresse, die in der Konfiguration des angeschlossenen Rechners als Default Gateway angegeben ist, nicht korrekt ist.

Netzwerk Modus → Stealth *(Werkseinstellung außer mGuard delta)*



Stealth-Konfiguration: automatisch / statisch / mehere Clients

automatisch

(Standard) Der mGuard analysiert den Netzwerkverkehr, der über ihn läuft, und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig und arbeitet transparent.

statisch

Wenn der mGuard keinen über ihn laufenden Netzwerkverkehr analysieren kann, z. B. weil zum lokal angeschlossenen Rechner nur Daten ein-, aber nicht ausgehen, dann muss die *Stealth-Konfiguration* auf **statisch** gesetzt werden. In diesem Fall stellt die Seite unten weitere Eingabefelder zur statischen Stealth-Konfiguration zur Verfügung.

mehrere Clients

Wie bei **automatisch**, es können jedoch mehr als nur ein Rechner am internen Interface (gesicherter Port) des mGuard angeschlossen sein und somit mehrere IP-Adressen am internen Interface (gesicherter Port) des mGuard verwendet werden.

In diesem Modus ist die VPN Funktionalität des mGuard aus technischen Gründen deaktiviert.

Stealth Management IP-Adresse (Netzwerk Modus = Stealth)

Hier können Sie eine weitere IP-Adresse angeben, über welche der mGuard administriert werden kann.

Wenn

- unter *Stealth-Konfiguration* die Option **mehrere Clients** gewählt ist oder
- der Client ARP Anfragen nicht beantwortet oder
- kein Client vorhanden ist,

dann ist der Fernzugang über HTTPS, SNMP und SSH nur über diese Adresse möglich.

IP-Adresse

Die zusätzliche IP-Adresse, unter welcher der mGuard erreichbar sein soll. Die IP-Adresse „0.0.0.0“ deaktiviert die Management IP-Adresse.

Netzmaske

Die Netzmaske zu obiger IP-Adresse.

Default Gateway

Das Default Gateway (= Standardgateway) des Netzes, in dem sich der mGuard befindet.

Verwende Management VLAN: Ja / Nein

Wenn die IP-Adresse innerhalb eines VLANs liegen soll, ist diese Option auf **Ja** zu setzen.

Management VLAN ID

Eine VLAN ID zwischen 1 und 4095.

☞ Eine Erläuterung des Begriffes „VLAN“ findet sich auf Seite 153.

Stealth Statische Stealth-Konfiguration (Stealth-Konfiguration = statisch)

IP-Adresse des Clients

Die IP-Adresse des Clients.

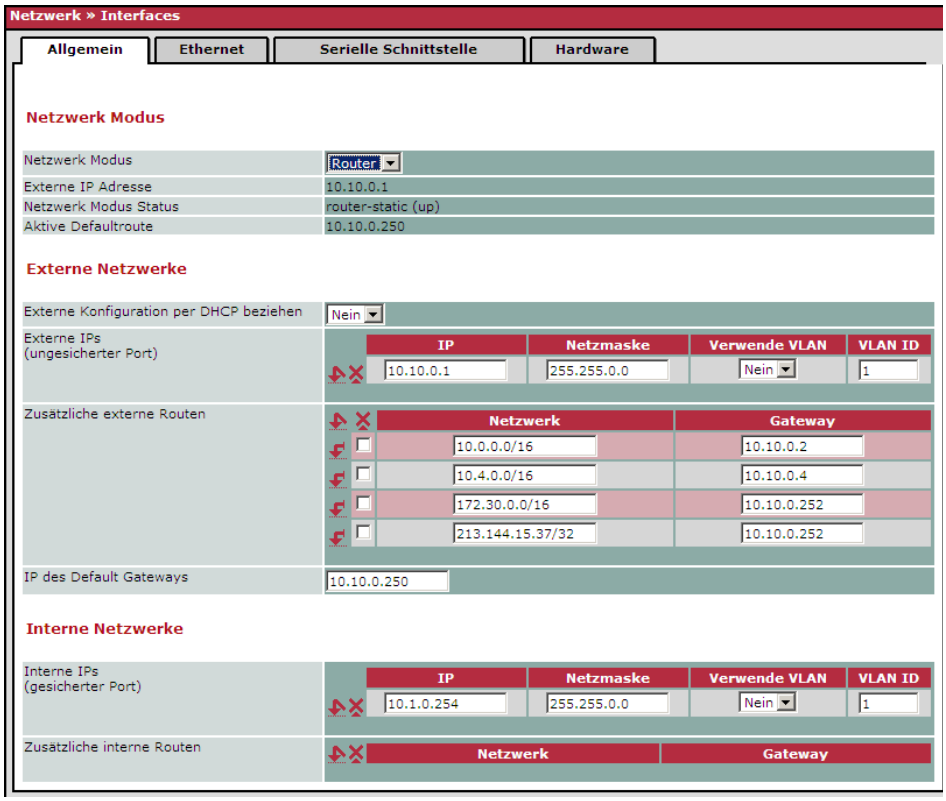
MAC-Adresse des Clients

Das ist die physikalische Adresse der Netzwerkkarte des lokalen Rechners, an dem der mGuard angeschlossen ist.

⌧Die MAC-Adresse ermitteln Sie wie folgt:
Auf der DOS-Ebene (**Menü Start, Alle Programme, Zubehör, Eingabeaufforderung)** folgenden Befehl eingeben:

```
ipconfig /all
```

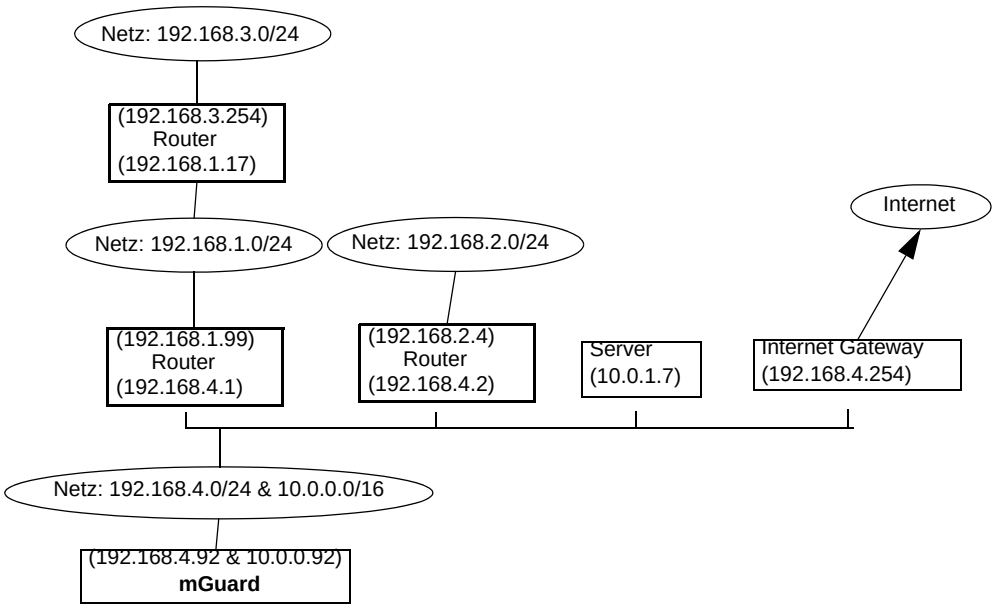
Netzwerk Modus → Router *(Werkseinstellung mGuard delta)*



Externe Netzwerke (Netzwerkmodus = Router)

Hier legen Sie fest, wie bestimmte Netze, die sich auf Seiten des externen Interface befinden, zu erreichen sind.

Beispiel:



Für das in der oben abgebildeten Beispielskizze würde man den mGuard wie folgt konfigurieren:

Externe IPs:

IP-Adresse	Netzmaske
192.168.4.92	255.255.255.0
10.0.0.92	255.255.0.0

Zusätzliche externe Routen:

Netzwerk	Gateway
192.168.2.0/24	192.168.4.2
192.168.1.0/24	192.168.4.1
192.168.3.0/24	192.168.4.1

IP des Default Gateway:
192.168.4.254

Externe Konfiguration per DHCP beziehen: Ja / Nein

☞ Falls der mGuard die Konfigurationsdaten per DHCP (Dynamic Host Configuration Protocol) vom DHCP-Server bezieht, legen Sie **Ja** fest. Dann bleiben gegebenfalls weitere bereits bestehende Angaben unter **Externe Netzwerke** wirkungslos, die entsprechenden Felder auf dieser Seite werden ausgeblendet.

☞ Falls der mGuard die Daten nicht per DHCP (Dynamic Host Configuration Protocol) vom DHCP-Server bezieht, legen Sie **Nein** fest und machen dann die folgenden Angaben:

Externe IPs (ungesicherter Port)

Die Adressen, unter denen der mGuard von Geräten des externen Netzes aus erreichbar ist. Sie bilden die Schnittstelle zu anderen Teilen des LAN oder zum Internet. Findet hier der Übergang zum Internet statt, werden die IP-Adressen vom Internet Service Provider (ISP) vorgegeben.

IP/Netzmaske

IP-Adresse und Netzmaske für das externe Interface (WAN).

Verwende VLAN: Ja / Nein

Wenn die IP-Adresse innerhalb eines VLANs liegen soll, ist diese Option auf **Ja** zu setzen.

VLAN ID

Eine VLAN ID zwischen 1 und 4095.

☞ Eine Erläuterung des Begriffes „VLAN“ findet sich auf Seite 153.

☞ Falls Sie Einträge aus der Liste löschen wollen: Der erste Eintrag kann nicht gelöscht werden.

Zusätzliche externe Routen

Zusätzlich zur Default Route (s. u.) können Sie weitere externe Routen festlegen.

Netzwerk / Gateway

Siehe auch „Netzwerk-Beispielskizze“ auf Seite 141.

IP des Default Gateways

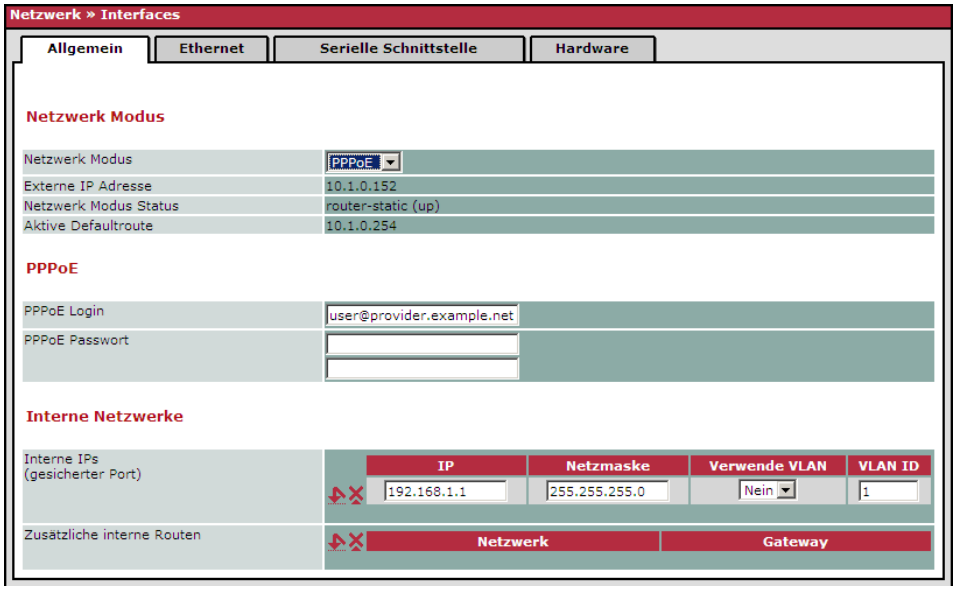
Wird vom Internet Service Provider (ISP) vorgegeben, wenn der mGuard den Übergang zum Internet herstellt. Wird der mGuard innerhalb des LANs ein-

gesetzt, wird die IP-Adresse des Default-Gateways vom Netzwerk-Administrator vorgegeben.

⌦ Diese Einstellung wird ignoriert, wenn eine lokale Default Route unter „Netzwerk Modus“ definiert wurde.

⌦ Wenn das lokale Netz dem externen Router nicht bekannt ist, z. B. im Falle einer Konfiguration per DHCP, dann sollten Sie unter Netzwerksicherheit → NAT Ihr lokales Netz angeben, also 0.0.0.0/0 (siehe „Netzwerksicherheit → NAT“ auf Seite 103)

Netzwerk Modus → PPPoE



PPPoE

Für Zugriffe ins Internet gibt der Internet Service Provider (ISP) dem Benutzer einen Benutzernamen (Login) und ein Passwort. Diese werden abfragt, wenn Sie eine Verbindung ins Internet herstellen wollen.

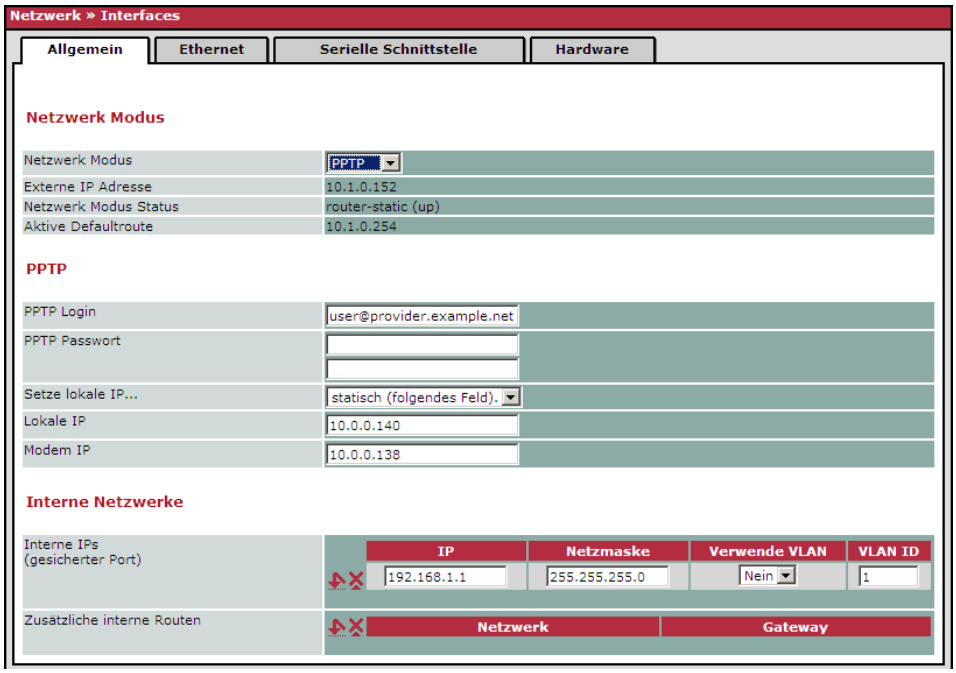
PPPoE Login

Benutzername (Login), den der Internet Service Provider (ISP) anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPPoE Passwort

Passwort, das der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

Netzwerk Modus → PPTP



PPTP

Für Zugriffe ins Internet gibt der Internet Service Provider (ISP) dem Benutzer einen Benutzernamen (Login) und ein Passwort. Diese werden abfragt, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPTP Login

Benutzername (Login), den der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPTP Passwort

Passwort, das der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

Setze lokale IP...: statisch / über DHCP

Bei Über DHCP:

Werden die Adressdaten für den Zugang zum PPTP-Server vom Internet Service Provider per DHCP geliefert, wählen Sie **Über DHCP**.

Dann ist kein Eintrag unter **Lokale IP** zu machen.

Modem IP. Das ist die Adresse des PPTP-Servers des Internet Service Providers.

Bei Statisch (folgendes Feld):

Werden die Adressdaten für den Zugang zum PPTP-Server nicht per DHCP vom Internet Service Provider geliefert, dann muss die IP-Adresse gegenüber dem PPTP-Server angegeben werden - als lokale IP-Adresse.

Lokale IP

IP-Adresse, unter der der mGuard vom PPTP-Server aus zu erreichen ist.

Modem IP

Das ist die Adresse des PPTP-Servers des Internet Service Providers.

Netzwerk Modus → Router, PPPoE oder PPTP

Interne Netzwerke

Interne IPs (gesicherter Port)

Interne IP ist die IP-Adresse, unter der der mGuard von Geräten des lokal angeschlossenen lokalen Netzes erreichbar ist.

Im **Router**- / **PPPoE**- / **PPTP**-Modus ist werksseitig voreingestellt:

IP-Adresse:	**192.168.1.1**
Lokale Netzmaske:	**255.255.255.0**

Sie können weitere Adressen festlegen, unter der mGuard von Geräten des lokal angeschlossenen Netzes angesprochen werden kann. Das ist zum Beispiel dann hilfreich, wenn das lokal angeschlossene Netz in Subnetze unterteilt wird. Dann können mehrere Geräte aus verschiedenen Subnetzen den mGuard unter unterschiedlichen Adressen erreichen.

IP

IP-Adresse, unter welcher der mGuard am internen Interface erreichbar sein soll.

Netzmaske

Die Netzmaske des am internen Interface angeschlossenen Netzes.

Verwende VLAN

Wenn die IP-Adresse innerhalb eines VLANs liegen soll, ist diese Option auf **Ja** zu setzen.

VLAN ID

Eine VLAN ID zwischen 1 und 4095.

☞ Eine Erläuterung des Begriffes „VLAN“ findet sich auf Seite 153.

☞ Falls Sie Einträge aus der Liste löschen wollen: Der erste Eintrag kann nicht gelöscht werden.

Zusätzliche interne Routen

Sind am lokal angeschlossen Netz weitere Subnetze angeschlossen, können Sie zusätzliche Routen definieren.

Netzwerk

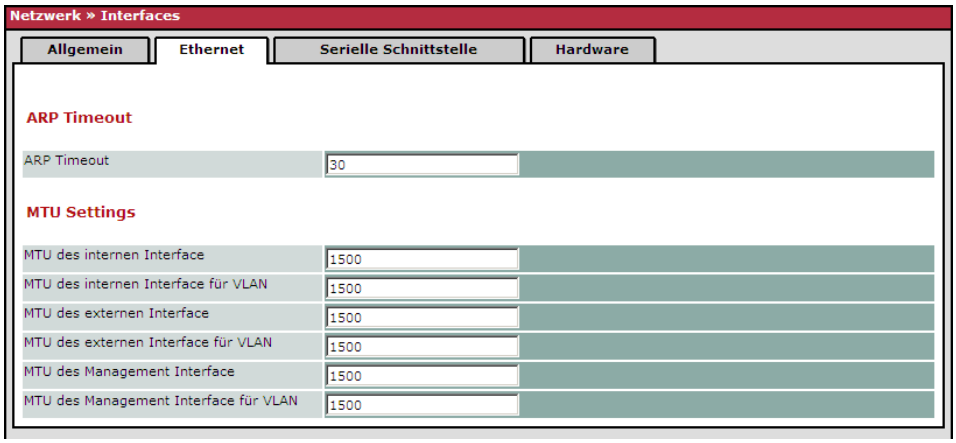
Das Netzwerk in CIDR-Schreibweise angeben - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140.

Gateway

Das Gateway, über welches dieses Netzwerk erreicht werden kann.

☞ Siehe auch „Netzwerk-Beispielskizze“ auf Seite 141. Mit einer internen Route nach 0.0.0.0/0 können Sie eine Default Route über das interne Interface definieren.

Ethernet



ARP Timeout

ARP Timeout

Lebensdauer der Einträge in der ARP-Tabelle.

MTU Settings

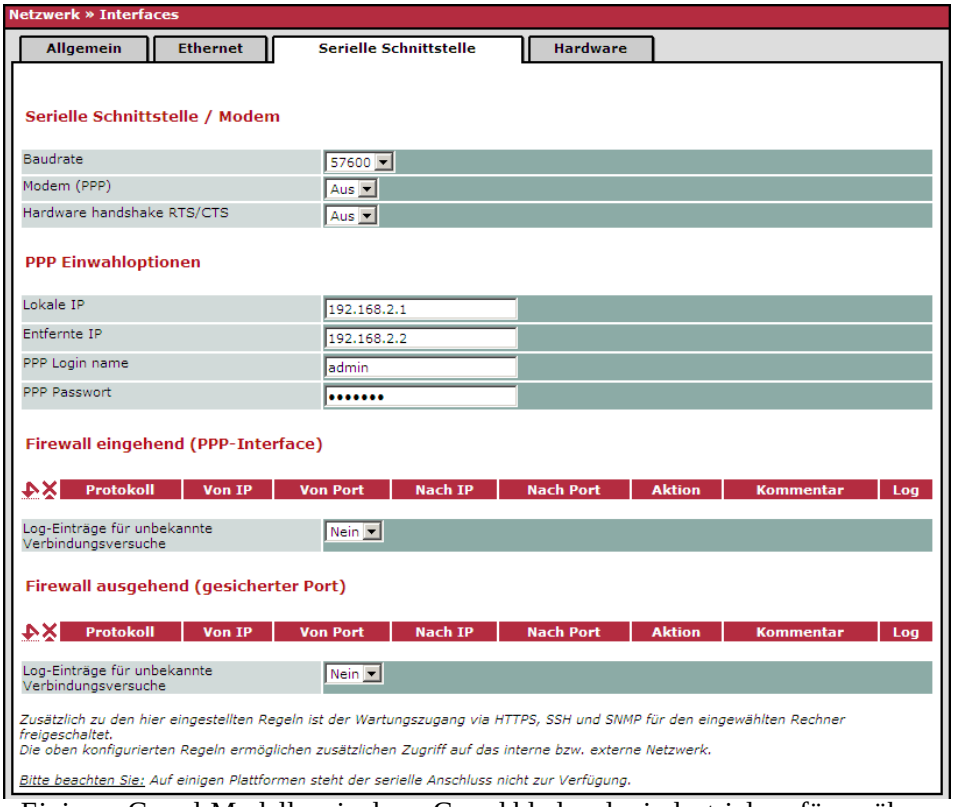
MTU des ... Interface

Die Maximum Transfer Unit (MTU) beschreibt die maximale IP-Paketlänge, die beim betreffenden Interface benutzt werden darf.

⌦ Bei VLAN-Interface:

Da die VLAN Pakete 4 Byte länger als Pakete ohne VLAN sind, haben bestimmte Treiber Probleme mit der Verarbeitung der größeren Pakete. Eine Reduzierung der MTU auf 1496 kann dieses Problem beseitigen.

Serielle Schnittstelle



Einige mGuard-Modelle wie der mGuard blade oder industrial verfügen über eine von außen zugängliche serielle Schnittstelle. Über diese kann man mit einem Terminalprogramms oder via PPP-Verbindung auf den mGuard zugreifen (PPP = Point-to-Point Protocol).

Serielle Schnittstelle / Modem

Baudrate

Über die Auswahlliste können Sie festlegen, mit welcher Übertrgungsgeschwindigkeit die serielle Schnittstelle arbeiten soll.

Modem (PPP): Aus / Ein

Wenn diese Option auf **Aus** steht, kann man sich über ein Terminal über den seriellen Port einloggen. Steht sie auf **Ein**, kann man sich per PPP-Protokoll auf dem mGuard einloggen.

Hardware handshake RTS/CTS: Aus / An

Bei **Ein** findet bei der PPP-Verbindung Flusssteuerung durch RTS- und CTS-Signale statt.

PPP Einwahloptionen

Lokale IP

IP-Adresse des mGuard, unter der er bei einer PPP-Verbindung erreichbar ist.

Entfernte IP

IP-Adresse der Gegenstelle von der PPP-Verbindung.

PPP Login name

Login, welchen die PPP-Gegenstelle angeben muss, um per PPP-Verbindung Zugriff auf den mGuard zu bekommen.

PPP Passwort

Das Passwort, welches die PPP-Gegenstelle angeben muss, um per PPP-Verbindung Zugriff auf den mGuard zu bekommen.

Firewall eingehend (PPP-Interface)

Firewallregeln für PPP-Verbindungen zum lokalen Ethernet-Interface (LAN). Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

Von / Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140.

Von / Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- ☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- ☞ oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche: Ja / Nein

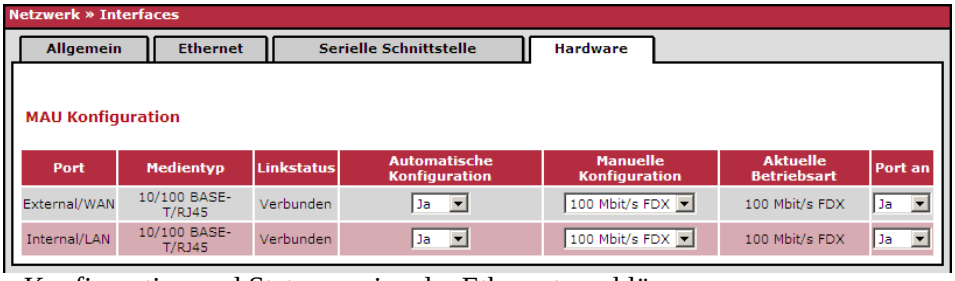
Bei **Ja** werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

Firewall ausgehend (gesicherter Port)

Firewallregeln für ausgehende PPP-Verbindungen vom lokalen Ethernet-Interface (LAN).

Die Parameter entsprechen denen von *Firewall eingehend (PPP-Interface)* - s. o.

Hardware



Konfiguration und Statusanzeige der Ethernetanschlüsse:

MAU Konfiguration

Port
Name des Ethernetanschlusses, auf welchen sich die Zeile bezieht.

Medientyp
Medientyp des Ethernetanschlusses.

Linkstatus
Up: Die Verbindung ist aufgebaut.
Down: Die Verbindung ist nicht aufgebaut.

Automatische Konfiguration: Ja / Nein
Ja: Versuche die benötigte Betriebsart eigenständig zu ermitteln.
Nein: Verwende die vorgegebene Betriebsart aus der Spalte „Manuelle Konfiguration“.

⌧ Beide Netzwerkschnittstellen des mGuard sind zur Verbindung mit einem Rechner konfiguriert. Beim Anschluss an einen Hub ist Folgendes zu beachten: Bei deaktivierter *Automatischer Konfiguration* wird auch die Auto-MDIX Funktion deaktiviert, d. h. der Port des mGuard muss entweder an den Uplink-Port des Hub oder mittels eines Cross-Link-Kabels mit dem Hub verbunden werden.

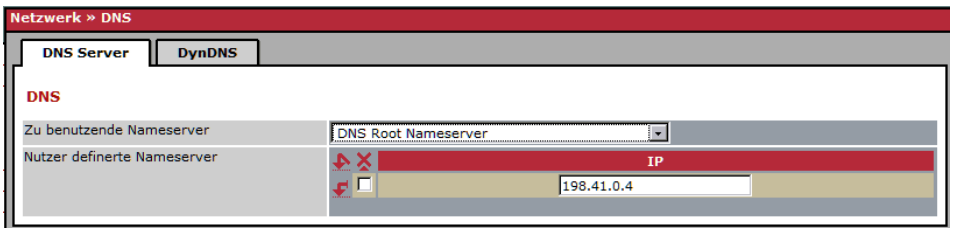
Manuelle Konfiguration
Die gewünschte Betriebsart, wenn *Automatische Konfiguration* auf *Nein* gestellt ist.

Aktuelle Betriebsart
Die aktuelle Betriebsart des Netzwerkanschlusses.

Port On: Ja / Nein *(nur mGuard industrial und smart)*
Schaltet den Ethernetanschluss ein und aus.

6.4.2 Netzwerk →DNS

DNS Server



Soll der mGuard eine Verbindung zu einer Gegenstelle aufbauen (z. B. VPN-Gateway oder NTP-Server), muss ihm die IP-Adresse dieser Gegenstelle bekannt

sein. Wird ihm die Adresse in Form eines Hostnamens angegeben (d. h. in der Form www.example.com), dann muss das Gerät auf einem Domain Name Server (DNS) nachschlagen, welche IP-Adresse sich hinter dem Hostnamen verbirgt. Wenn sich der mGuard nicht im *Stealth*-Modus befindet, können Sie die lokal angeschlossenen Clients so konfigurieren, dass sie den mGuard zur Auflösung von Hostnamen in IP-Adressen benutzen können. Siehe „IP-Konfiguration bei Windows-Clients“ auf Seite 94

DNS

Zu benutzende Nameserver

Möglichkeiten:

- DNS Root Nameserver
- Provider definiert (z. B. via PPPoE oder DHCP)
- Nutzer definiert (unten stehende Liste)

DNS Root Nameserver:

Anfragen werden an die Root-Nameserver im Internet gerichtet, deren IP-Adressen im mGuard gespeichert sind. Diese Adressen ändern sich selten.

Provider definiert (z. B. via PPPoE oder DHCP)

Es wird der Domain Name Server des Internet Service Providers benutzt, der den Zugang zum Internet zur Verfügung stellt. Wählen Sie diese Einstellung nur dann, wenn der mGuard im *PPPoE*-, im *PPTP*-Modus oder im *Router*-Modus mit DHCP arbeitet.

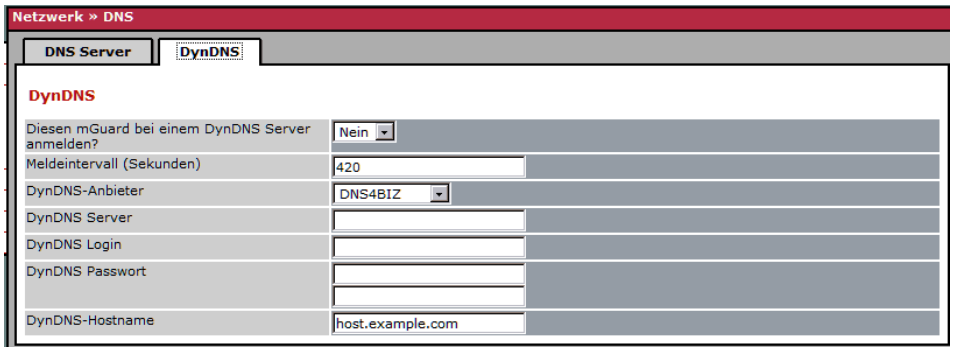
Nutzer definiert (unten stehende Liste)

Ist diese Einstellung gewählt, nimmt der mGuard mit den Domain Name Servern Verbindung auf, die in der Liste *Nutzer definierte Nameserver* aufgeführt sind.

Nutzer definierte Nameserver

In dieser Liste können Sie die IP-Adressen von Domain Name Servern erfassen. Soll einer von diesen vom mGuard benutzt werden, muss oben unter **Zu benutzende Nameserver** die Option *Nutzer definiert (unten stehende Liste)* eingestellt sein..

DynDNS



Zum Aufbau von VPN-Verbindungen muss mindestens die IP-Adresse eines der Partner bekannt sein, damit diese miteinander Kontakt aufnehmen können. Diese Bedingung ist nicht erfüllt, wenn beide Teilnehmer ihre IP-Adressen dynamisch von ihrem Internet Service Provider zugewiesen bekommen. In diesem Fall kann aber ein DynDNS-Service wie z. B. DynDNS.org oder DNS4BIZ.com helfen.

Bei einem DynDNS-Service wird die jeweils gültige IP-Adresse unter einem festen Namen registriert.
Sofern Sie für einen vom mGuard unterstützten DynDNS-Service registriert sind, können Sie in diesem Dialogfeld die entsprechenden Angaben machen.

Diesen mGuard bei einem DynDNS Server anmelden? Ja / Nein

Wählen Sie **Ja**, wenn Sie beim DynDNS-Anbieter entsprechend registriert sind, und der mGuard den Service benutzen soll. Dann meldet der mGuard die aktuelle IP-Adresse, die gerade dem eigenen Internet-Anschluss vom Internet Service Provider zugewiesen ist, an den DynDNS Service.

Meldeintervall (Sekunden)

Standard: 420 (Sekunden).

Immer wenn sich die IP-Adresse des eigenen Internet-Anschlusses ändert, informiert der mGuard den DynDNS Service über die neue IP-Adresse. Aus Zuverlässigkeitsgründen erfolgt diese Meldung zusätzlich in dem hier festgelegten Zeitintervall.

Bei einigen DynDNS Anbietern wie z.B. DynDNS.org hat diese Einstellung keine Wirkung, da dort ein zu häufiges Melden zur Löschung des Accounts führen kann.

DynDNS Anbieter

Die zur Auswahl gestellten Anbieter unterstützen das Protokoll, das auch der mGuard unterstützt.

Wählen Sie den Namen des Anbieters aus, bei dem Sie registriert sind, z. B. DynDNS.org, TinyDynDNS, DNS4BIZ

DynDNS Server

Name des Servers des oben ausgewählten DynDNS-Anbieters.

DynDNS Login, DynDNS Passwort

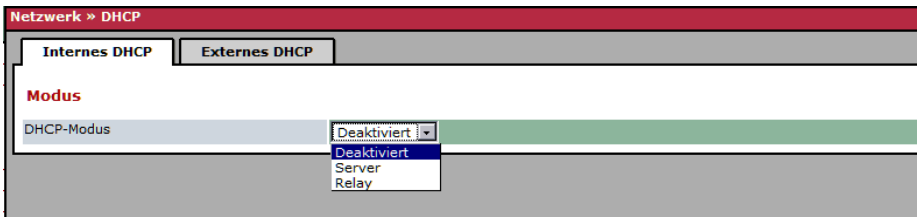
Geben Sie hier den Benutzernamen und das Passwort ein, das Ihnen vom DynDNS-Anbieter zugeteilt worden ist.

DynDNS Hostname

Der für diesen mGuard gewählte Hostname beim DynDNS-Service - sofern Sie einen DynDNS-Dienst benutzen und oben die entsprechenden Angaben gemacht haben. Unter diesem Hostnamen ist dann Ihr Rechner, der am mGuard angeschlossen ist, erreichbar.

6.4.3 Netzwerk →DHCP

Mit dem Dynamic Host Configuration Protocol (DHCP) kann den direkt am mGuard angeschlossenen Clients automatisch die hier eingestellte Netzwerkkonfiguration zugeteilt werden. Unter *Internes DHCP* können Sie DHCP Einstellungen für das interne Interface (LAN) vornehmen und unter *Externes DHCP* die DHCP Einstellungen für das externe Interface (WAN).



Modus

DHCP-Modus: Deaktiviert / Server / Relay

Setzen Sie diesen Schalter auf **Server**, wenn der mGuard als eigenständiger DHCP Server arbeiten soll.

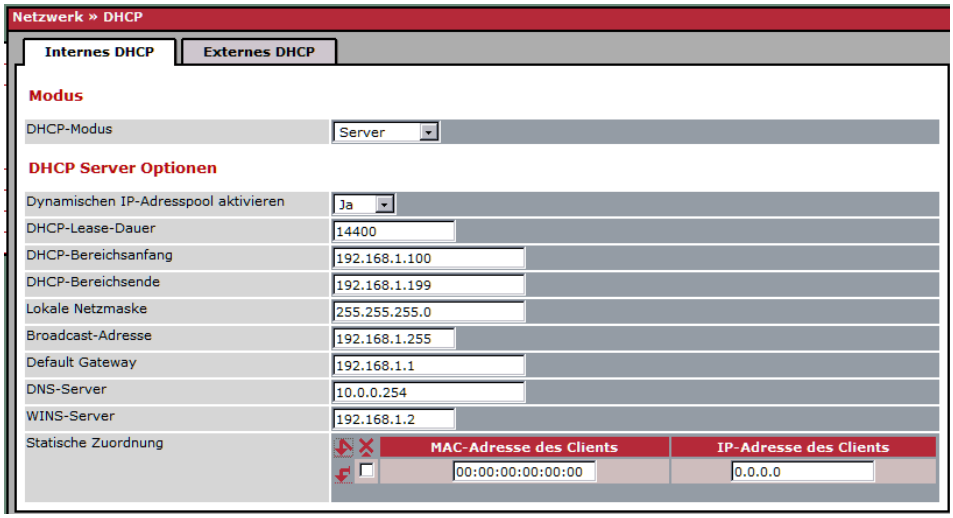
Setzen Sie ihn auf **Relay**, wenn der mGuard DHCP Anfragen an einen anderen DHCP Server weiterleiten soll.

Steht der Schalter auf **Deaktiviert**, beantwortet der mGuard keine DHCP Anfragen.

⌦ Der DHCP Server/Relay funktioniert auch im *Stealth* Modus.

Ist als DHCP-Modus *Server* ausgewählt, werden unten auf der Seite entsprechende Einstellmöglichkeiten wie folgt eingeblendet.

DHCP-Modus →Server:



DHCP Server Optionen

Dynamischen IP-Adresspool aktivieren: Ja / Nein

Setzen Sie diesen Schalter auf **Ja**, wenn sie den weiter unten durch *DHCP-Bereichsanfang* bzw. *DHCP-Bereichsende* angegebenen IP-Adresspool verwenden wollen (siehe unten).

Setzen Sie diesen Schalter auf **Nein**, wenn nur statische Zuweisungen anhand der MAC-Adresse vorgenommen werden sollen (siehe unten).

DHCP-Lease-Dauer

Zeit in Sekunden, für die eine dem Client zugeteilte Netzwerkkonfiguration gültig ist. Kurz vor Ablauf dieser Zeit sollte ein Client seinen Anspruch auf die ihm zugeteilte Konfiguration erneuern. Ansonsten wird diese u.U. anderen Rechnern zugeteilt.

Bei aktiviertem dynamischen IP-Adresspool:

Bei aktiviertem DHCP-Server und aktiviertem dynamischem IP-Adresspool können Sie die Netzwerkparameter angeben, die vom Client benutzt werden sollen:

DHCP-Bereichsanfang: **DHCP-Bereichsende:**	Anfang und Ende des Adressbereichs, aus dem der DHCP-Server des mGuard den lokal angeschlossenen Clients IP-Adressen zuweisen soll.

Lokale Netzmaske:	Legt die Netzmaske der Clients fest. Voreingestellt ist: 255.255.255.0
Broadcast-Adresse:	Legt die Broadcast-Adresse der Clients fest.
Default Gateway:	Legt fest, welche IP-Adresse beim Client als Default-Gateway benutzt wird. In der Regel ist das die interne IP-Adresse des mGuard.
DNS-Server:	Adresse des Servers, bei dem Clients über den Domain Name Service (DNS) Hostnamen in IP-Adressen auflösen lassen können. Wenn der DNS-Dienst des mGuard genutzt werden soll, dann die interne IP-Adresse des mGuards angeben.
WINS-Server:	Adresse des Servers, bei dem Clients über den Windows Internet Naming Service (WINS) Hostnamen in Adressen auflösen können.

Statische Zuordnung [anhand der MAC-Adresse]

Die MAC-Adresse Ihres Clients finden Sie wie folgt heraus:
Windows 95/98/ME: Starten Sie **winipcfg** in einer DOS-Box
Windows NT/2000/XP: Starten Sie **ipconfig /all** in einer Eingabeaufforderung. Die MAC-Adresse wird als „Physikalische Adresse“ angezeigt.
Linux: Rufen Sie in einer Shell **/sbin/ifconfig** oder **ip link show** auf .

Bei den Angaben haben Sie folgende Möglichkeiten:

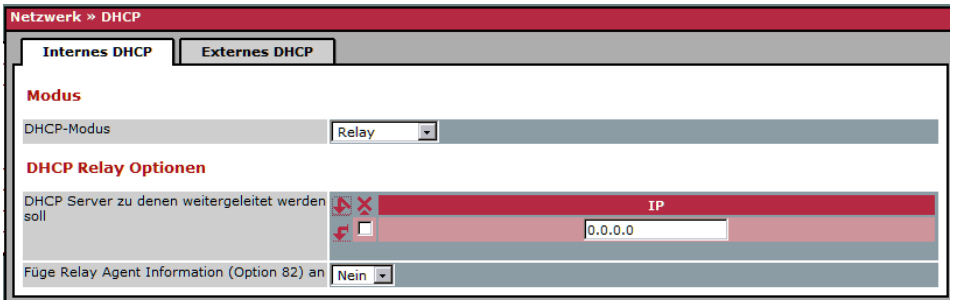
MAC-Adresse des Clients
Die MAC-Adresse (ohne Leerzeichen oder Bindestriche) des Clients.

IP-Adresse des Clients
Die statische IP des Clients, die der MAC-Adresse zugewiesen werden soll.

- ☞ Die statischen Zuweisungen haben Vorrang vor dem dynamischen IP-Adresspool.
- ☞ Statische Zuweisungen dürfen sich nicht mit dem dynamischen IP-Adresspool überlappen.
- ☞ Eine IP darf nicht in mehreren statischen Zuweisungen verwendet werden, ansonsten wird diese IP-Adresse mehreren MAC-Adressen zugeordnet.
- ☞ Es sollte nur ein DHCP-Server pro Subnetz verwendet werden.

Ist als DHCP-Modus *Relay* ausgewählt, werden unten auf der Seite entsprechende Einstellmöglichkeiten wie folgt eingeblendet.

DHCP-Modus →Relay



DHCP Relay Optionen

DHCP Server, zu denen weitergeleitet werden soll

Eine Liste von einem oder mehreren DHCP Servern, an welche DHCP Anfragen weitergeleitet werden sollen.

Füge Relay Agent Information (Option 82) an: Ja / Nein

Beim Weiterleiten können zusätzliche Informationen nach RFC 3046 für die DHCP Server angefügt werden, an welche weitergeleitet wird.

⌦ IP-Konfiguration bei Windows-Clients

Wenn Sie den DHCP-Server des mGuard starten, können Sie die lokal angeschlossenen Clients so konfigurieren, dass sie ihre IP-Adressen automatisch beziehen.

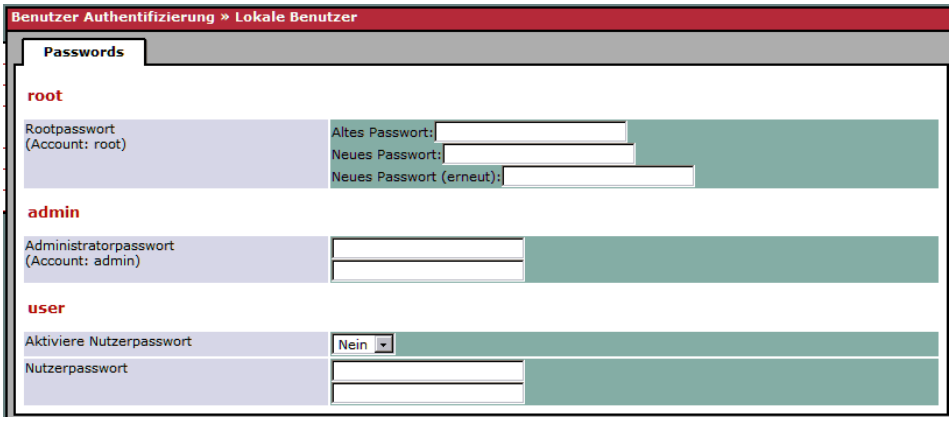
Dazu klicken Sie unter Windows XP **Start, Systemsteuerung, Netzwerkverbindungen**: Symbol des LAN-Adapters mit der rechten Maustaste klikken und im Kontextmenü **Eigenschaften** klicken. Im Dialogfeld *Eigenschaften von LAN-Verbindung* lokales Netz auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag **Internetprotokoll (TCP/IP)** markieren und dann die Schaltfläche **Eigenschaften** klicken.

Im Dialogfeld *Eigenschaften von Internetprotokoll (TCP/IP)* die gebotenen Angaben bzw. Einstellungen machen.

6.5 Menü Benutzerauthentifizierung

6.5.1 Benutzerauthentifizierung →Lokale Benutzer

Passwords



Der mGuard bietet 3 Stufen von Benutzerrechten. Um sich auf der entsprechenden Stufe anzumelden, muss der Benutzer das Passwort angeben, das der jeweiligen Berechtigungsstufe zugeordnet ist.

Berechtigungsstufe	
Root	Bietet vollständige Rechte für alle Parameter des mGuard. Hintergrund: Nur diese Berechtigungsstufe erlaubt es, sich per SSH so mit dem Gerät zu verbinden, dass man das ganze System auf den Kopf stellen kann. Dann kann man es nur noch mit „Flashen“ der Firmware in seinen Auslieferungszustand zurückbringen (siehe „Flashen der Firmware“ auf Seite 143). Voreingestelltes Rootpasswort: **root**
Administrator	Bietet die Rechte für die Konfigurationsoptionen, die über die webbasierte Administratoroberfläche zugänglich sind. Voreingestellter Benutzername: **admin** Voreingestelltes Passwort: **mGuard** Der Benutzername **admin** kann nicht geändert werden.
Nutzer	Ist ein Nutzerpasswort festgelegt und aktiviert, dann muss der Benutzer nach jedem Neustart des mGuard bei Zugriff auf eine beliebige HTTP URL dieses Passwort angeben, damit VPN-Verbindungen möglich sind. Wollen Sie diese Option nutzen, legen Sie im entsprechenden Eingabefeld das Nutzerpasswort fest. (Hinweis: Solange ein erforderlicher Nutzerlogin nicht erfolgt ist, sind evtl. auch einige andere Dienste auf dem mGuard nicht gestartet oder lassen sich nicht einwandfrei umkonfigurieren.)

root

Rootpasswort (Account: root)
Werksseitig voreingestellt: **root**
Wollen Sie das Rootpasswort ändern, geben Sie ins Feld *Altes Passwort* das alte Passwort ein, in die beiden Felder darunter das neue gewünschte Passwort.

admin

Administratorpasswort (Account: admin)
Werksseitig voreingestellt: **mGuard**
(unveränderbarer Benutzername: admin)

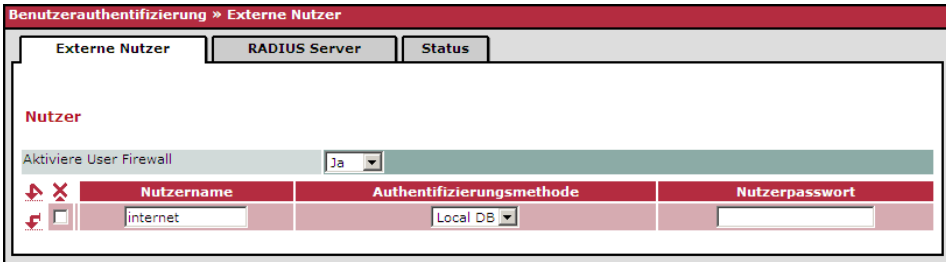
user

Aktiviere Nutzerpasswort: Nein / Ja
Werksseitig ist Nutzer-Passwortschutz ausgeschaltet.
Ist unten ein Nutzerpasswort festgelegt, kann der Nutzer-Passwortschutz mit diesem Schalter aktiviert bzw. deaktiviert werden.

Nutzerpasswort
Werkseitig ist kein Nutzerpasswort voreingestellt. Um eines festzulegen, geben Sie in beide Eingabefelder übereinstimmend das gewünschte Passwort ein.

6.5.2 Benutzerauthentifizierung →Externe Benutzer

Remote Users



Nutzer

Liste der externen Benutzer: deren Benutzername und Authentifizierungsmethode

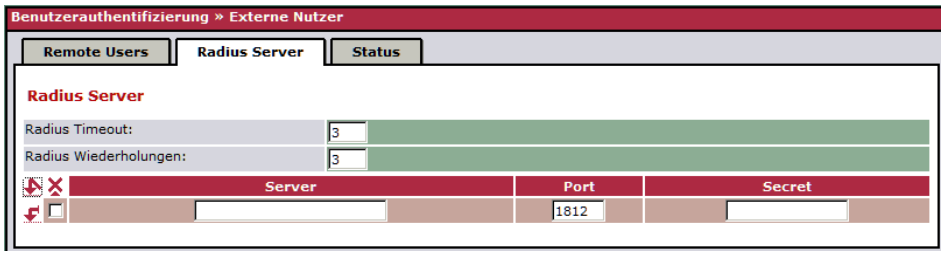
Aktiviere User Firewall: Ja / Nein
Unter dem Menüpunkt *Benutzerfirewall* können Firewall-Regeln definiert werden, die dort bestimmten externen Nutzern zugeordnet werden.
Mit **Ja** legen Sie fest, dass die den unten aufgelisteten Benutzern zugeordneten Firewallregeln in Kraft gesetzt werden, sobald sich betreffende Benutzer anmelden.

Nutzername
Name des Benutzers

Authentifizierungsmethode: Radius / Local
Local:
In der Spalte *Nutzerpasswort* muss das Passwort eingetragen werden, das dem Benutzer zugeordnet ist

Radius:
Meldet sich ein Benutzer mit seinem Passwort an, übermittelt der mGuard das von ihm angegebene Passwort zwecks Überprüfung dem Radius Server. Fällt die Prüfung positiv aus, erhält der Benutzer Zugang.

Radius Server



Radius Server

Radius Timeout
Legt fest (in Sekunden), wie lange der mGuard auf die Antword des Radius Servers wartet. Standard: 3 (Sekunden)

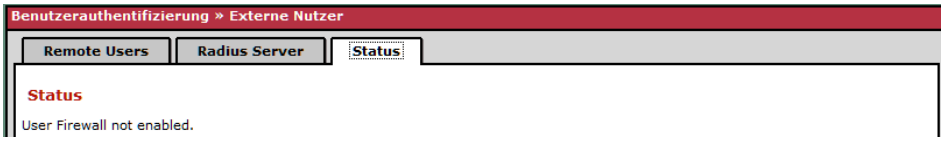
Radius Wiederholungen:
Legt fest, wie oft bei Überschreitung des Radius Timeout Anfragen an den Radius Server wiederholt werden. Standard: 3

Server
Name des Servers oder IP-Adresse

Port
Vom Radius Server benutze Port-Nummer

Secret
Server-Passwort

Status



Bei aktivierter Benutzerfirewall wird hier deren Status angezeigt.

6.6 Menü Netzwerksicherheit (nicht blade Controller)

6.6.1 Netzwerksicherheit → Packet Filter

Der mGuard beinhaltet eine *Stateful Packet Inspection Firewall*. Die Verbindungsdaten einer aktiven Verbindung werden in einer Datenbank erfasst (connection tracking). Dadurch sind Regeln nur für eine Richtung zu definieren, Daten aus der anderen Richtung einer Verbindung, und nur diese, werden automatisch durchgelassen. Ein Nebeneffekt ist, dass bestehende Verbindungen bei einer Umkonfiguration nicht abgebrochen werden, selbst wenn eine entsprechende neue Verbindung nicht mehr aufgebaut werden dürfte.

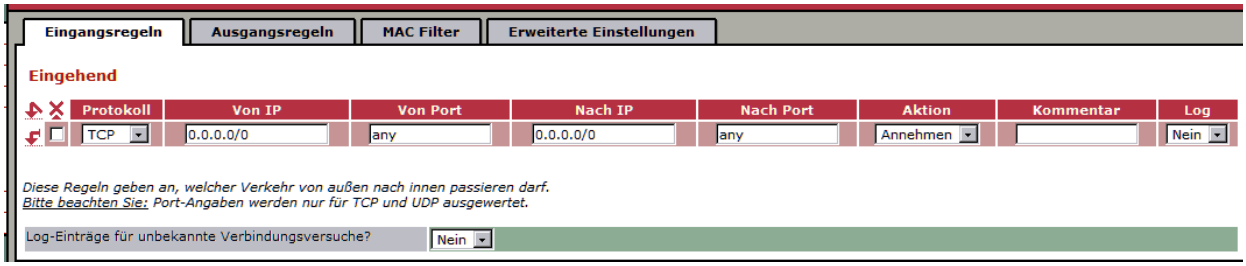
Werkseitige Voreinstellung der Firewall:

- Alle eingehenden Verbindungen werden abgewiesen (außer VPN).
- Die Datenpakete aller ausgehenden Verbindungen werden durchgelassen.

⌧ VPN-Verbindungen unterliegen nicht den unter diesem Menüpunkt festgelegten Firewall-Regeln. Firewall-Regeln für jede einzelne VPN-Verbindung können Sie unter Menü **VPN → Verbindungen** festlegen.

⌧ Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

Eingangsregeln



Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenverbindungen, die von extern initiiert wurden.
Ist keine Regel gesetzt, werden alle eingehenden Verbindungen (außer VPN) verworfen (= Werkseinstellung).

⌧ Durch die Aktivierung der Antivirusfunktion (siehe „Web-Sicherheit →HTTP“ auf Seite 111, „Web-Sicherheit →FTP“ auf Seite 113, „E-Mail-Sicherheit →POP3“ auf Seite 116, „E-Mail-Sicherheit →SMTP“ auf Seite 119) werden implizit Firewallregeln für die Protokolle HTTP, FTP, SMTP und POP3 eingerichtet, die **nicht** in der Liste der Firewall-Regeln erscheinen.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

Von IP / Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Adressenbereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140.

Von Port / Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen (s. u.).)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

⌧ Im Stealth-Modus entspricht **Abweisen** der Aktion **Verwerfen**.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

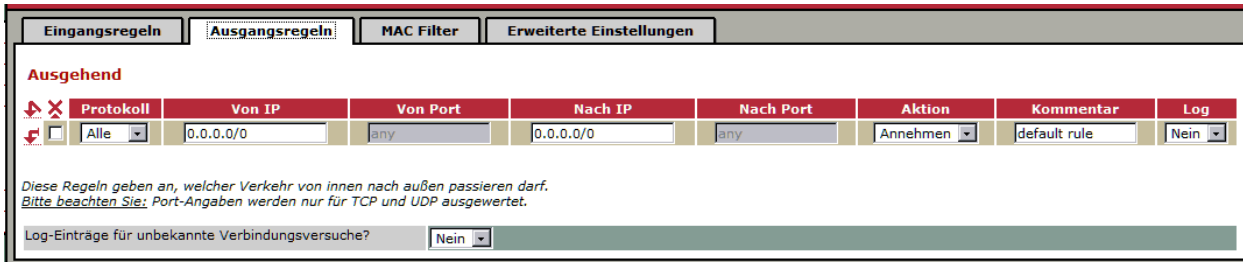
Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche: Ja / Nein

Bei **Ja** werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden. (Werksseitige Voreinstellung: **Nein**)

Ausgangsregeln



Listet die eingerichteten Firewall-Regeln auf. Sie gelten für ausgehende Datenverbindungen, die von intern initiiert wurden, um mit einer entfernten Gegenstelle zu kommunizieren.

Werkseinstellung: Per Werkseinstellung ist eine Regel gesetzt, die alle ausgehenden Verbindungen zulässt.

Ist keine Regel gesetzt, sind alle ausgehenden Verbindungen verboten (außer VPN).

⌧ Durch die Aktivierung der Antivirusfunktion (siehe „Web-Sicherheit →HTTP“ auf Seite 111, „Web-Sicherheit →FTP“ auf Seite 113, „E-Mail-Sicherheit →POP3“ auf Seite 116, „E-Mail-Sicherheit →SMTP“ auf Seite 119) werden implizit Firewallregeln für die Protokolle HTTP, SMTP und POP3 eingerichtet, die **nicht** in der Liste der Firewall-Regeln erscheinen.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

Von IP / Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Adressenbereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140.

Von Port / Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen (s. u.).)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

⌦ Im Stealth-Modus entspricht **Abweisen** der Aktion **Verwerfen**.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

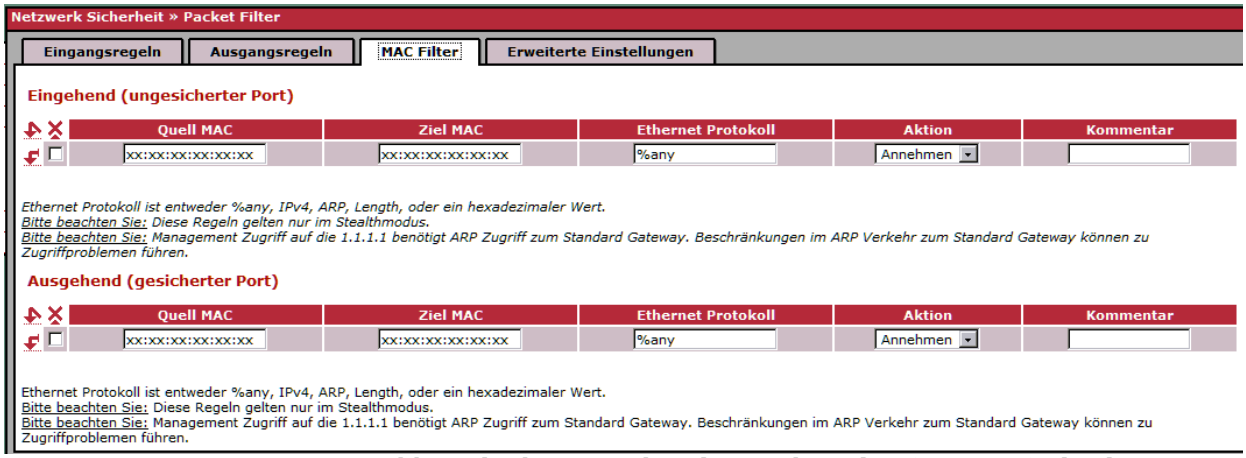
Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche: Ja / Nein

Bei **Ja** werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden. (Werksseitige Voreinstellung: **Nein**)

MAC Filter


Netzwerk Sicherheit » Packet Filter
Eingangsregeln
Ausgangsregeln
MAC Filter
Erweiterte Einstellungen
Eingehend (ungesicherter Port)
Quell MAC
Ziel MAC
Ethernet Protokoll
Aktion
Kommentar
xx:xx:xx:xx:xx:xx
xx:xx:xx:xx:xx:xx
%any
Annehmen
Ethernet Protokoll ist entweder %any, IPv4, ARP, Length, oder ein hexadezimaler Wert.
Bitte beachten Sie: Diese Regeln gelten nur im Stealthmodus.
Bitte beachten Sie: Management Zugriff auf die 1.1.1.1 benötigt ARP Zugriff zum Standard Gateway. Beschränkungen im ARP Verkehr zum Standard Gateway können zu Zugriffproblemen führen.
Ausgehend (gesicherter Port)
Quell MAC
Ziel MAC
Ethernet Protokoll
Aktion
Kommentar
xx:xx:xx:xx:xx:xx
xx:xx:xx:xx:xx:xx
%any
Annehmen
Ethernet Protokoll ist entweder %any, IPv4, ARP, Length, oder ein hexadezimaler Wert.
Bitte beachten Sie: Diese Regeln gelten nur im Stealthmodus.
Bitte beachten Sie: Management Zugriff auf die 1.1.1.1 benötigt ARP Zugriff zum Standard Gateway. Beschränkungen im ARP Verkehr zum Standard Gateway können zu Zugriffproblemen führen.

Im *Stealth* Modus können neben dem Packet Filter (Layer 3/4), der den Datenverkehr z. B. nach ICMP Nachrichten oder TCP/UDP Verbindungen filtert, zusätzlich MAC Filter (Layer 2) gesetzt werden. Ein MAC Filter (Layer 2) filtert nach MAC Adressen und Ethernet Protokollen.

Im Gegensatz zum Packet Filter ist der MAC Filter stateless. Das heißt, werden Regeln eingeführt, müssen gegebenenfalls entsprechende Regeln für die Gegenrichtung ebenfalls erstellt werden.

Ist keine Regel gesetzt, sind alle ARP und IP Packete erlaubt.

- Achten Sie auf die Hinweise auf dem Bildschirm, wenn Sie MAC Filter Regeln setzen.
- Die hier angegebenen Regeln haben Vorrang gegenüber den Packet Filter Regeln.

Quell MAC

Angabe der Quell MAC Adresse: xx:xx:xx:xx:xx:xx steht für alle MAC Adressen.

Ziel MAC

Angabe der Ziel MAC Adresse: xx:xx:xx:xx:xx:xx steht für alle MAC Adressen. Der Wert ff:ff:ff:ff:ff:ff ist die Broadcast MAC Adresse, an die z. B. alle ARP Anfragen geschickt werden.

Ethernet Protokoll

%any steht für alle Ethernet Protokolle. Weitere Protokolle können mit dem Namen oder in HEX angegeben werden, zum Beispiel:

- IPv4 oder 0800
- ARP oder 0806

Aktion

Annehmen bedeutet, die Datenpackete dürfen passieren

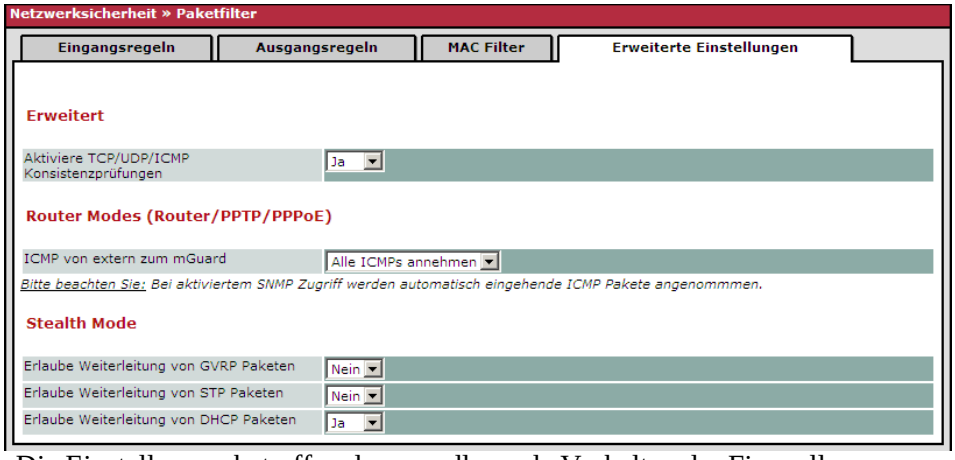
Verwerfen bedeutet, die Datenpackete werden verworfen

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

☞ Der MAC Filter unterstützt keine Logging Funktionalität

Erweiterte Einstellungen



Die Einstellungen betreffen das grundlegende Verhalten der Firewall.

Erweitert

Aktiviere TCP/UDP/ICMP Konsistenzprüfungen: Ja / Nein

Wenn auf **Ja** gesetzt, führt der mGuard eine Reihe von Tests auf falsche Prüfsummen, Paketgrößen, usw. durch und verwirft Pakete, die die Tests nicht bestehen.

Werkseitig ist dieser Schalter auf **Ja** gesetzt.

Router Modes (Router / PPTP / PPPoE)

ICMP von extern zum mGuard

Mit dieser Option können Sie das Verhalten beim Empfang von ICMP-Nachrichten beeinflussen, die aus dem externen Netz an den mGuard gesendet werden. Sie haben folgende Möglichkeiten:

Verwerfen: Alle ICMP-Nachrichten zum mGuard werden verworfen.

Annehmen von Ping: Nur Ping-Nachrichten (ICMP Typ 8) zum mGuard werden akzeptiert.

Alle ICMPs annehmen: Alle Typen von ICMP Nachrichten zum mGuard werden akzeptiert.

Stealth Modus

Erlaube Weiterleitung von GVRP Paketen: Ja / Nein

Das GARP VLAN Registration Protocol (GVRP) wird von GVRP fähigen Switches verwendet, um Konfigurationsinformationen miteinander auszutauschen.

Ist dieser Schalter auf **Ja** gesetzt, dann können GVRP Pakete den mGuard im *Stealth* Modus passieren.

Erlaube Weiterleitung von STP Paketen: Ja / Nein

Das Spawning-Tree Protocol (STP) (802.1d) wird von Bridges und Switches verwendet, um Schleifen in der Verkabelung zu entdecken und zu berücksichtigen.

Ist dieser Schalter auf **Ja** gesetzt, dann können STP Pakete den mGuard im *Stealth* Modus passieren.

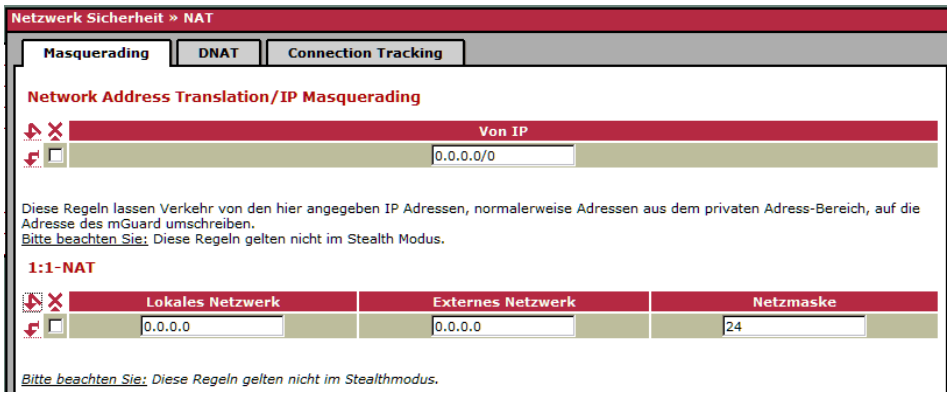
Erlaube Weiterleitung von DHCP Paketen: Ja / Nein

Bei **Ja** wird dem Client erlaubt, über DHCP eine IP-Adresse zu beziehen - unabhängig von den Firewallregeln für ausgehenden Datenverkehr.

Die Voreinstellung für diesen Schalter ist **Ja**.

6.6.2 Netzwerksicherheit → NAT

Masquerading



Network Address Translation / IP Masquerading

Listet die festgelegten Regeln für NAT (**N**etwork **A**ddress **T**ranslation) auf.

Das Gerät kann bei ausgehenden Datenpaketen die angegebenen Absender-IP-Adressen aus seinem internen Netzwerk auf seine eigene externe Adresse umschreiben, eine Technik, die als NAT (Network Address Translation) bezeichnet wird.

Diese Methode wird benutzt, wenn die internen Adressen extern nicht geroutet werden können oder sollen, z. B. weil ein privater Adressbereich wie 192.168.x.x oder die interne Netzstruktur verborgen werden soll.

Dieses Verfahren wird auch *IP-Masquerading* genannt.

- Arbeitet der mGuard im *PPPoE/PPTP*-Modus, muss NAT aktiviert werden, um Zugriff auf das Internet zu erhalten. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.
- Bei der Verwendung von mehreren statischen IP-Adressen für das externe Interface wird immer die erste IP-Adresse der Liste für IP-Masquerading verwendet.

Werkseinstellung: Es findet kein NAT statt.

Bei den Angaben haben Sie folgende Möglichkeiten:

Von IP

0.0.0.0/0 bedeutet alle Adressen, d. h. alle internen IP-Adressen werden dem NAT-Verfahren unterzogen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140

1:1-NAT

Listet die festgelegten Regeln für 1:1 NAT (**N**etwork **A**ddress **T**ranslation) auf. Dabei spiegelt der mGuard die Adressen des internen Netzes in das externe Netz.

Beispiel:
Der mGuard befindet sich mit seiner internen Schnittstelle im Netzwerk 192.168.0.0/24 und mit seiner externen Schnittstelle im Netzwerk 10.0.0.0/24. Durch das 1:1 NAT läßt sich der Rechner 192.168.0.8 im externen Netz unter der IP-Adresse 10.0.0.8 erreichen.

192.168.0.0/24 **10.0.0.0/24**

Werkseinstellung: Es findet kein 1:1 NAT statt.

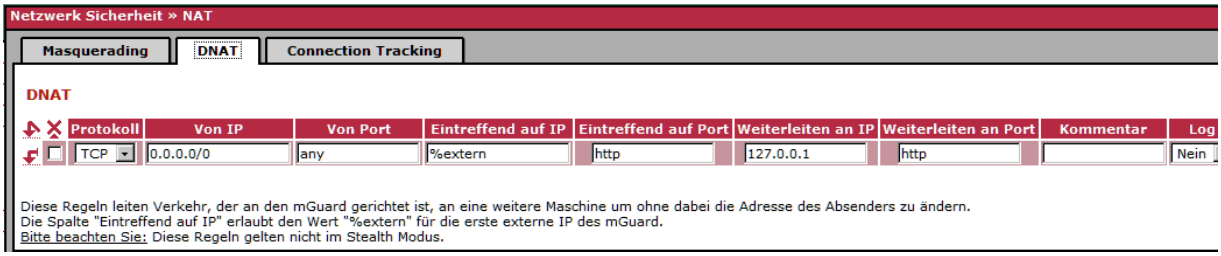
Bei den Angaben haben Sie folgende Möglichkeiten:

Lokales Netzwerk
Die Netzwerkadresse am lokalen Interface (LAN).

Externes Netzwerk
Die Netzwerkadresse am externen Interface (WAN).

Netzmaske
Die Netzmaske als Wert zwischen 1 und 32 für die lokale und externe Netzwerkadresse (siehe auch „CIDR (Classless InterDomain Routing)“ auf Seite 140).

DNAT



(DNT = Destination-NAT)
Listet die festgelegten Regeln zur Port-Weiterleitung auf.
Bei Port-Weiterleitung geschieht Folgendes: Der Header eingehender Datenpakete aus dem externen Netz, die an die externe IP-Adresse (oder eine der externen IP-Adressen) des mGuard sowie an einen bestimmten Port des mGuard gerichtet sind, werden so umgeschrieben, dass sie ins interne Netz an einen bestimmten Rechner und zu einem bestimmten Port dieses Rechners weitergeleitet werden. D. h. die IP-Adresse und Port-Nummer im Header eingehender Datenpakete werden geändert.
Dieses Verfahren wird auch Destination-NAT genannt.

⌧ Die hier eingestellten Regeln haben Vorrang gegenüber den Einstellungen unter **Netzwerk Sicherheit**, **Packet Filter → Eingehend**.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll: TCP / UDP
Geben Sie hier das Protokoll an, auf den sich die Regel beziehen soll.

Von IP

Absenderadresse, für die Weiterleitungen durchgeführt werden sollen.

0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140.

Von Port

Absenderport, für den Weiterleitungen durchgeführt werden sollen.

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben, z. B. 110 für pop3 oder pop3 für 110.

Geben Sie hier das Protokoll an, auf den sich die Regel beziehen soll.

Eintreffend auf IP

Geben Sie hier die externe IP-Adresse (oder eine der externen IP-Adressen) des mGuard an.

ODER

Falls ein dynamischer Wechsel der externen IP-Adresse des mGuard erfolgt, so dass diese nicht angebbar ist, verwenden Sie folgende Variable: **%extern.**

☒ Die Angabe von **%extern** bezieht sich bei der Verwendung von mehreren statischen IP-Adressen für das externe Interface immer auf die erste IP-Adresse der Liste.

Eintreffend auf Port

Original-Ziel-Port, der in eingehenden Datenpaketen angegeben ist.

Sie können nur einzelne Ports angeben, entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen: (z. B. 110 für pop3 oder pop3 für 110).

Weiterleiten an IP

Interne IP-Adresse, an die die Datenpakete weitergeleitet werden sollen und auf die die Original-Zieladressen umgeschrieben werden.

Weiterleiten an Port

Port, an den die Datenpakete weitergeleitet werden sollen und auf den die Original-Port-Angaben umgeschrieben werden.

Sie können nur einzelne Ports angeben, entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen: (z. B. 110 für pop3 oder pop3 für 110).

Kommentar

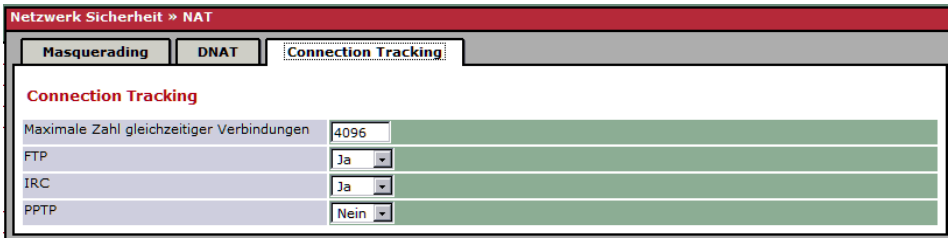
Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Port-Weiterleitungs-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Connection Tracking



Connection Tracking

Maximale Zahl gleichzeitiger Verbindungen

Dieser Eintrag legt eine Obergrenze fest. Diese ist so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht wird. Bei Angriffen kann sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie den Wert erhöhen.

FTP: Ja / Nein

Wird beim FTP-Protokoll eine ausgehende Verbindung hergestellt, um Daten abzurufen, gibt es zwei Varianten der Datenübertragung: Beim „aktiven FTP“ stellt der angerufene Server im Gegenzug eine zusätzliche Verbindung zum Anrufer her, um auf dieser Verbindung die Daten zu übertragen. Beim „passiven FTP“ baut der Client diese zusätzliche Verbindung zum Server zur Datenübertragung auf. Damit die zusätzlichen Verbindungen von der Firewall durchgelassen werden, muss **FTP** auf **Ja** stehen (Standard).

IRC: Ja / Nein

Ähnlich wie bei FTP: Beim Chatten im Internet per IRC müssen nach aktivem Verbindungsaufbau auch eingehende Verbindungen zugelassen werden, soll das Chatten reibungslos funktionieren. Damit diese von der Firewall durchgelassen werden, muss **IRC** auf **Ja** stehen (Standard).

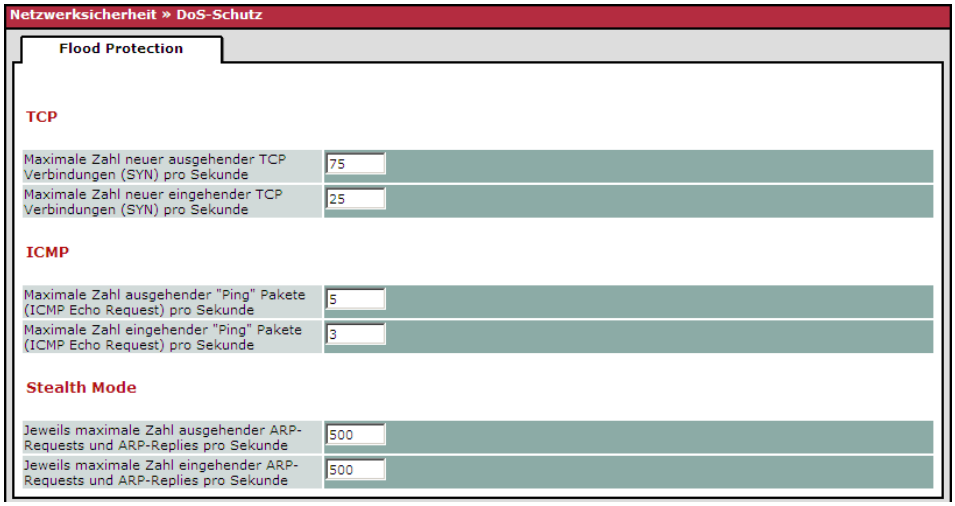
PPTP: Ja / Nein

Muss **Ja** gesetzt werden, wenn von lokalen Rechnern ohne Zuhilfenahme des mGuard VPN-Verbindungen mittels PPTP zu externen Rechner aufgebaut werden können sollen.

Werkseitig ist dieser Schalter auf **Nein** gesetzt.

6.6.3 Netzwerksicherheit → DoS-Schutz

Flood Protection


Netzwerksicherheit » DoS-Schutz
Flood Protection
TCP
Maximale Zahl neuer ausgehender TCP Verbindungen (SYN) pro Sekunde
75
Maximale Zahl neuer eingehender TCP Verbindungen (SYN) pro Sekunde
25
ICMP
Maximale Zahl ausgehender "Ping" Pakete (ICMP Echo Request) pro Sekunde
5
Maximale Zahl eingehender "Ping" Pakete (ICMP Echo Request) pro Sekunde
3
Stealth Mode
Jeweils maximale Zahl ausgehender ARP-Requests und ARP-Replies pro Sekunde
500
Jeweils maximale Zahl eingehender ARP-Requests und ARP-Replies pro Sekunde
500

TCP

Maximale Zahl neuer ausgehender TCP Verbindungen (SYN) pro Sekunde
Werkseinstellung: 75

Maximale Zahl neuer eingehender TCP Verbindungen (SYN) pro Sekunde

Werkseinstellung: 25

Diese beiden Einträge legen Maximalwerte für die zugelassenen ein- und ausgehenden TCP-Verbindungen pro Sekunde fest. Diese sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

ICMP

Maximale Zahl ausgehender "Ping" Pakete (ICMP Echo Request) pro Sekunde
Werkseinstellung: 5

Maximale Zahl eingehender "Ping" Pakete (ICMP Echo Request) pro Sekunde
Werkseinstellung: 3

Diese beiden Einträge legen Maximalwerte für die zugelassenen ein- und ausgehenden "Ping"-Pakete pro Sekunde fest. Diese sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

Stealth Mode

Jeweils maximale Zahl ausgehender ARP-Requests und ARP-Replies pro Sekunde
Werkseinstellung: 500

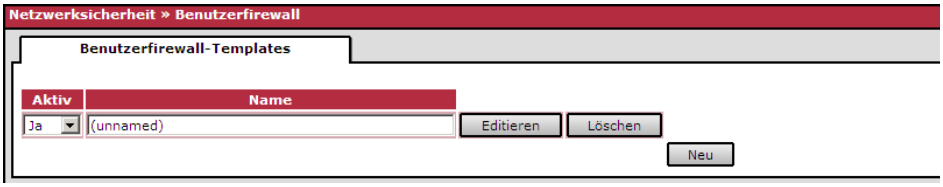
Jeweils maximale Zahl eingehender ARP-Requests und ARP-Replies pro

Sekunde
Werkseinstellung: 500

Diese beiden Einträge legen Maximalwerte für die zugelassenen ein- und ausgehenden ARP-Requests pro Sekunde fest. Diese sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

6.6.4 Netzwerksicherheit → Benutzerfirewall

Benutzerfirewall-Templates



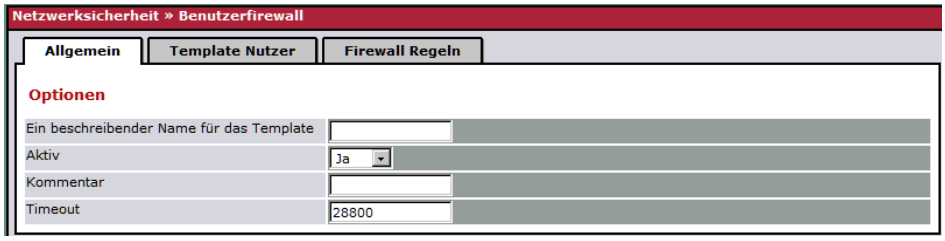
Hier werden alle definierten User Firewall Templates aufgelistet.

- **Definierte User Firewall Template aktivieren / deaktivieren**:
  Parameter **Aktiv** auf **Ja** bzw. **Nein** setzen.
- **Definierte User Firewall Template bearbeiten**:
  Neben dem Listeneintrag auf die Schaltfläche **Editieren** klicken.
- **Definierte User Firewall Template löschen**:
  Neben dem Listeneintrag auf die Schaltfläche **Löschen** klicken.
- **Neue User Firewall Template definieren**:
  1. auf die Schaltfläche **Neu** klicken.
     Folge: Die angezeigte Liste der User Firewall Templates erhält einen weiteren Eintrag.
  2. Neben diesem Listeneintrag die Schaltfläche **Editieren** klicken.

6.6.5 Benutzerfirewall → Template definieren

Nach Klicken auf **Editieren** erscheint folgende Seite:

Allgemein



Optionen

Ein beschreibender Name für das Template

Sie können das User Firewall Template frei benennen bzw. umbenennen.

Aktiv: Ja / Nein

Bei **Ja** ist das User Firewall Template aktiv, sobald sich externe Benutzer beim mGuard anmelden, die auf der Registerkarte *Template Nutzer* (s. u.) erfasst sind und denen Firewall-Regeln zugeordnet sind. Es spielt keine Rolle, von welchem Rechner und unter welcher IP sich ein Benutzer anmeldet. Die Zuordnung Benutzer - Firewall-Regeln erfolgt über die Authentifizierungsdaten, die der Benutzer bei seiner Anmeldung angibt (Benutzername, Passwort).

Kommentar

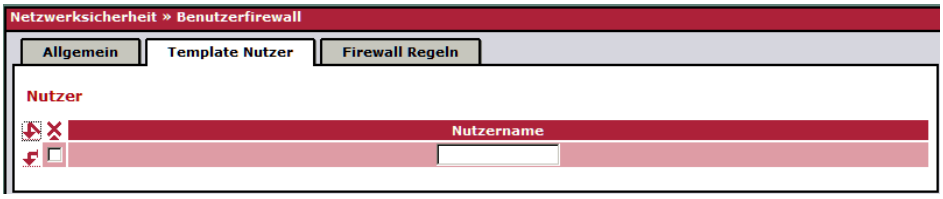
Optional: erläuternder Text

Timeout

Standard: 28800.

Gibt an in Sekunden, wann die die Firewall-Regeln außer Kraft gesetzt wird. Dauert die Sitzung des betreffenden Benutzers länger als die hier festgelegte Timeout-Zeit, muss er sich neu anmelden.

Template Nutzer

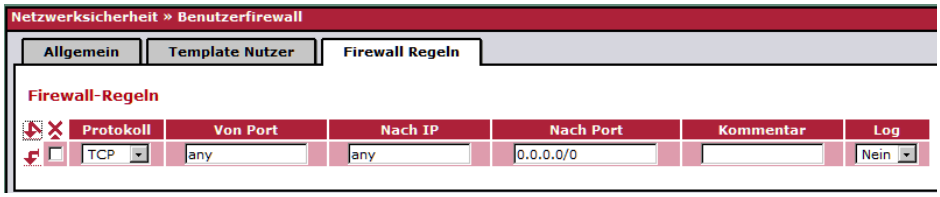


Nutzer

Nutzername

Geben Sie die Namen von Nutzern an. Die Namen müssen denen entsprechen, die Benutzerauthentifizierung → Externe Nutzer festgelegt sind - siehe „Benutzerauthentifizierung →Externe Benutzer“ auf Seite 96

Firewall Regeln



Firewall-Regeln

- Sind für einen Nutzer mehrere Firewall-Regeln definiert und aktiviert, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.
- Im *Stealth*-Modus ist in den Firewall-Regeln für den Client die wirkliche IP-Adresse zu verwenden oder aber auf 0.0.0.0/0 zu belassen, da nur ein Client durch den Tunnel angesprochen werden kann.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

Von Port/Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

6.7 Menü Web-Sicherheit (nicht blade Controller)

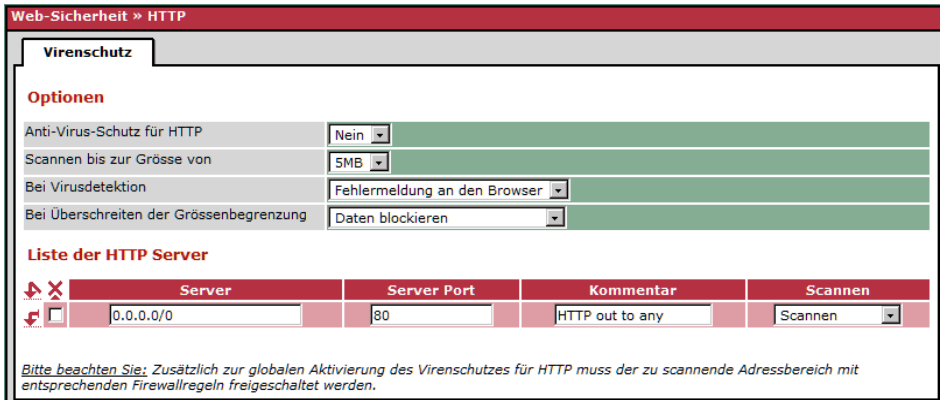
6.7.1 Web-Sicherheit →HTTP

Voraussetzungen:

Folgende Voraussetzungen müssen für die Nutzung des Virenfilters erfüllt sein:

- Installierte Antiviren-Lizenz. Die Anleitung, wie Sie eine Lizenz anfordern und installieren, finden Sie im Abschnitt „Verwaltung →Update“ auf Seite 58.
- Zugriff auf einen Update-Server mit den aktuellen Versionen der Virensignaturen (siehe Abschnitt „Verwaltung →Update“ auf Seite 58).

Virenschutz



Das HTTP-Protokoll wird von Web-Browsern zur Übertragung von Webseiten genutzt, hat aber noch viele andere Anwendungen. So wird es z. B. auch zum Download von Dateien wie z. B. Software-Updates oder zur Initialisierung von Multimedia-Streams genutzt.

Die Weiterleitung einer übertragenen Datei erfolgt erst, nachdem sie komplett geladen und überprüft wurde. Deshalb kann es bei größeren Dateien oder einer langsamen Download-Geschwindigkeit zu Verzögerungen in der Reaktionszeit der Benutzer-Software kommen.

⌧ Um den Anti-Virus-Schutz für HTTP zu testen, bietet sich zunächst der ungefährliche Eicar-Testvirus an, der eigens für Testzwecke unter der Adresse http://www.eicar.org/anti_virus_test_file.htm heruntergeladen werden kann.

Optionen

Anti-Virus-Schutz für HTTP: Ja / Nein

Bei **Ja** wird eine Port-Redirection für HTTP-Verbindungen auf den HTTP-Proxy angelegt.

Scannen bis zur Grösse von

Voreingestellt: 5 MB. Hier geben Sie die Maximalgröße der zu überprüfenden Dateien an.

Wird diese Grenze überschritten, wird eine Fehlermeldung an den Browser gesendet oder automatisch in den Durchlassmodus geschaltet.

Wenn die Speicherkapazität des mGuard nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an die Client-Software (Browser, Download-Manager) des Benutzers ausgegeben und ein Eintrag im Antivirus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, den Download zu einem späteren Zeitpunkt zu wiederholen

- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlassmodus aktivieren.

Bei Virusdetektion

Fehlermeldung an den Browser

Erkennt der Virenfilter einen Virus innerhalb eines Datentransfers vom HTTP-Server zum HTTP-Client, dann wird eine Fehlermeldung an den HTTP-Client gesendet. Die Darstellung dieser Fehlermeldung hängt vom jeweiligen HTTP-Client ab. Ein Webbrowser wird die Fehlermeldung in Form einer HTML-Seite darstellen. Ist eine innerhalb einer HTML-Seite nachgeladene Datei - z.B. eine Bilddatei - infiziert, so wird diese Datei im Browser nicht angezeigt. Wird ein Dateidownload per HTTP mittels Download-Manager vorgenommen, so wird die Fehlermeldung im Download-Manager angezeigt.

Bei Überschreiten der Grössenbegrenzung

Daten ungescannt durchlassen

Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlassmodus, wenn die eingestellte Dateigröße überschritten wird.

☞ In diesem Fall wird nicht auf Viren überprüft!

Daten blockieren

Diese Option bewirkt den Abbruch des Downloads und die Ausgabe eines Fehlercodes an die Client-Software.

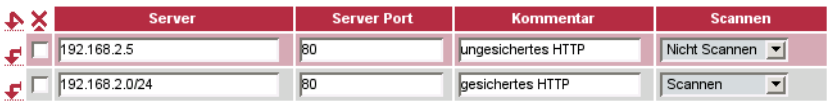
Liste der HTTP Server

Sie können die Server auswählen, deren Datenverkehr gefiltert werden soll und für jede IP explizit angeben, ob der Antivirus-Schutz aktiviert werden soll oder nicht. Dadurch ist auch die Angabe von „trusted“ Servern möglich.

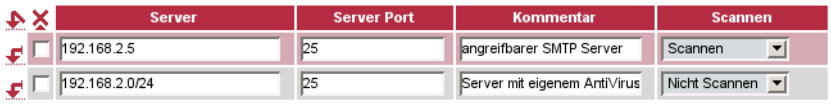
Beispiele:

Globale Aktivierung des Antivirus-Schutzes für HTTP:

Scan eines Subnetzes, Ausklammerung eines „trusted“ HTTP-Servers:



Scan eines einzelnen „untrusted“ HTTP-Servers in einem Subnetz:



⌦ Um den Anti-Virus-Schutz für HTTP- bzw. „FTP over HTTP“-Datenverkehr über einen Proxy zu aktivieren, fügen Sie eine neue Zeile in die Liste der Server ein und ersetzen den voreingestellten Port 80 durch den Proxy Port, welcher in Ihrem Webbrowser eingestellt ist.
Gebräuchliche Proxy-Portnummern sind 3128 und 8080.

⌦ Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach un-

ten abgearbeitet, die Reihenfolge der Regeln ist also ausschlaggebend für das Ergebnis.

⌦ Der Virenfilter kann parallel nur eine begrenzte Anzahl gleichzeitiger Verbindungen zu Mail-, HTTP- und FTP-Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. der Datenverkehr aller HTTP-Server wird gefiltert. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140.

⌦ Da ein Verbindungswunsch zunächst durch den Proxy entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert, da der Proxy nur Anfragen an die in der Liste angegebenen Adressen entgegennimmt.

Server Port

Hier geben Sie bitte die Nummer des Ports für das HTTP-Protokoll an. Der HTTP-Standardport **80** ist bereits voreingestellt.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Scannen

Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

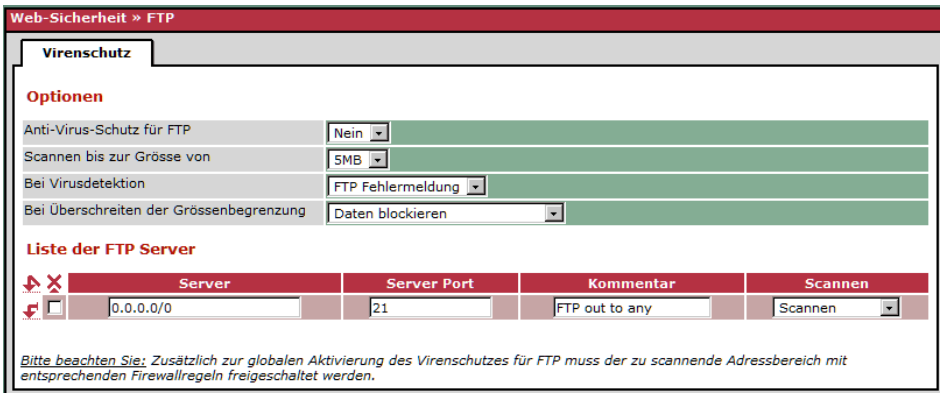
6.7.2 Web-Sicherheit →FTP

Voraussetzungen:

Folgende Voraussetzungen müssen für die Nutzung des Virenfilters erfüllt sein:

- Installierte Antiviren-Lizenz. Die Anleitung, wie Sie eine Lizenz anfordern und installieren, finden Sie im Abschnitt „Verwaltung →Update“ auf Seite 58.
- Zugriff auf einen Update-Server mit den aktuellen Versionen der Virensignaturen (siehe Abschnitt „Verwaltung →Update“ auf Seite 58).

Virenschutz



Das FTP-Protokoll wird zum Down- oder Upload von Dateien genutzt.

- Die Weiterleitung einer übertragenen Datei erfolgt erst, nachdem sie komplett geladen und überprüft wurde. Deshalb kann es bei größeren Dateien oder einer langsamen Download-Geschwindigkeit zu Verzögerungen in der Reaktionszeit der Benutzer-Software kommen.
- Um den Anti-Virus-Schutz für FTP zu testen, bietet sich zunächst der ungefährliche Eicar-Testvirus an, der eigens für Testzwecke unter der Adresse http://www.eicar.org/anti_virus_test_file.htm heruntergeladen werden kann.
- Der mGuard kann nur zum Schutz des FTP-Client genutzt werden.

Optionen

Anti-Virus-Schutz für FTP: Ja / Nein

Bei **Ja** wird eine Port-Redirection für FTP-Verbindungen auf den FTP-Proxy angelegt.

Scannen bis zur Grösse von

Voreingestellt: 5 MB. Hier geben Sie die Maximalgröße der zu überprüfenden Dateien an.

Wird diese Grenze überschritten, wird eine Fehlermeldung an den Client gesendet oder automatisch in den Durchlassmodus geschaltet.

Wenn die Speicherkapazität des mGuard nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an die Client-Software des Benutzers ausgegeben und ein Eintrag im Antivirus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, den Download/Upload zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlassmodus aktivieren.

Bei Virusdetektion

FTP Fehlermeldung

Erkennt der Virenfilter einen Virus innerhalb eines Datentransfers zwischen FTP-Server und FTP-Client, dann wird eine Fehlermeldung an den FTP-Client gesendet. Die Darstellung dieser Fehlermeldung hängt vom jeweiligen FTP-Client ab.

Bei Überschreiten der Grössenbegrenzung

Daten ungescannt durchlassen

Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlassmodus, wenn die eingestellte Dateigröße überschritten wird.

☒ In diesem Fall wird nicht auf Viren überprüft!

Daten blockieren

Diese Option bewirkt den Abbruch des Downloads und die Ausgabe eines Fehlercodes an die Client-Software.

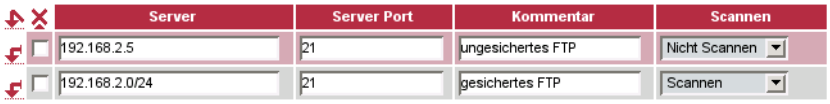
Liste der FTP Server

Sie können die Server auswählen, deren Datenverkehr gefiltert werden soll und für jede IP explizit angeben, ob der Antivirus-Schutz aktiviert werden soll oder nicht. Dadurch ist auch die Angabe von „trusted“ Servern möglich.

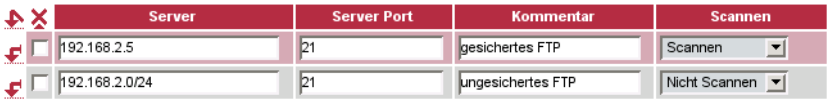
Beispiele:

Globale Aktivierung des Antivirus-Schutzes für FTP:

Scan eines Subnetzes, Ausklammerung eines „trusted“ FTP-Servers:



Scan eines einzelnen „untrusted“ FTP-Servers in einem Subnetz:



- Um den Anti-Virus-Schutz für FTP-Datenverkehr über einen Proxy zu aktivieren, fügen Sie eine neue Zeile in die Liste der Server ein und ersetzen den voreingestellten Port 21 durch den Proxy Port.
- Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also ausschlaggebend für das Ergebnis.
- Der Virenfilter kann parallel nur eine begrenzte Anzahl gleichzeitiger Verbindungen zu Mail-, HTTP- und FTP Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.
- Das Einschalten des FTP Virenfilters öffnet die Firewall für die entsprechenden Ports unabhängig von zusätzlichen anderslautenden Firewall-Regeln.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. der Datenverkehr aller FTP-Server wird gefiltert. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140.

- Da ein Verbindungswunsch zunächst durch den Proxy entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert, da der Proxy nur Anfragen an die in der Liste angegebenen Adressen entgegennimmt.

Server Port

Hier geben Sie bitte die Nummer des Ports für das FTP-Protokoll an. Der FTP-Standardport **21** ist bereits voreingestellt.

- Das Einschalten des FTP Virenfilters öffnet die Firewall für die entsprechenden Ports - unabhängig von zusätzlichen anderslautenden Firewall-Regeln.

Scannen

Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

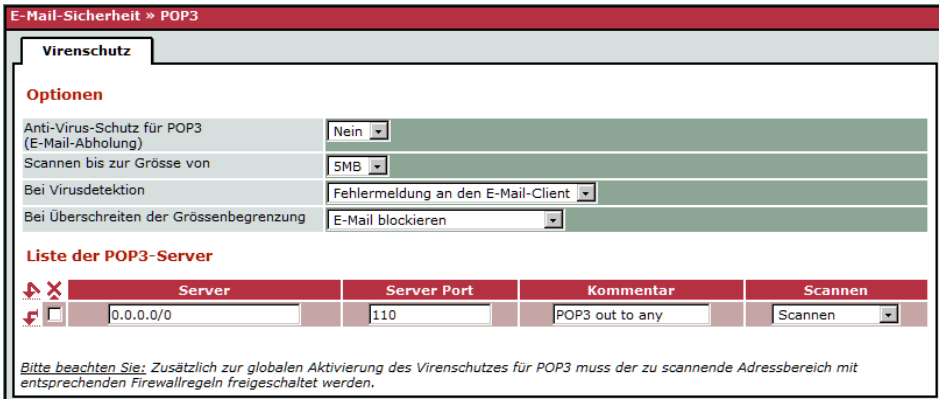
Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

6.8 Menü E-Mail-Sicherheit (nicht blade Controller)

6.8.1 E-Mail-Sicherheit →POP3

Virenschutz



Das POP3-Protokoll wird von Ihrem E-Mail-Client zum Empfang von E-Mails genutzt

- Der Virenfilter kann nur unverschlüsselte Daten auf Viren untersuchen. Deshalb sollten Sie Verschlüsselungsoptionen wie STLS oder SSL nicht aktivieren. Die verschlüsselte Authentifizierung mittels AUTH ist dagegen nutzbar, da die eigentliche Übertragung der E-Mail unverschlüsselt erfolgt.
- Bei Aktivierung des Virenschutzes für POP3 E-Mail-Empfang muss unter "Liste der POP3-Server" durch eine entsprechende Firewallregel der Adressbereich des/der entsprechenden POP3-Server freigeschaltet werden.

Optionen

Anti-Virus-Schutz für POP3 (E-Mail-Abholung): Ja / Nein

Bei **Ja** wird eine Port-Redirection für POP3-Verbindungen auf den POP3-Proxy angelegt.

Tipp: Bei einer POP3-Verbindung rufen die meisten E-Mail-Clients alle E-Mails über eine einzige Verbindung ab. Darum kann eine neue Einstellung erst greifen, wenn der E-Mail Transfer der aktuellen Verbindung vollzogen ist. Falls während eines laufenden E-Mail-Transfers die Einstellungen geändert werden sollen, müssen Sie den laufenden Transfer erst abbrechen, damit die neue Einstellunge greifen kann.

Scannen bis zur Grösse von

Voreingestellt: 5 MB. Hier geben Sie die Maximalgröße der zu überprüfenden Dateien an.

Wird diese Grenze überschritten, wird abhängig von der Einstellung „bei Überschreiten der Größenbegrenzung“ eine Fehlermeldung an den E-Mail-Client gesendet und die E-Mail nicht empfangen oder automatisch in den Durchlassmodus geschaltet.

Wenn die Speicherkapazität des mGuard nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an den E-Mail Client des Benutzers ausgegeben und ein Eintrag im Antivirus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, das Abholen der E-Mail zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren

- Sie können die Option für den automatischen Durchlassmodus aktivieren.

☞ Bitte beachten Sie, dass die Größe des Anhangs je nach Kodierung u.U. ein Vielfaches der ursprünglichen Dateigröße sein kann.

Bei Virusdetektion

Benachrichtigung per E-Mail
Erkennt der Virenfilter einen Virus, dann wird der Empfänger durch eine E-Mail benachrichtigt.

Fehlermeldung an den E-Mail Client
Erkennt der Virenfilter einen Virus, dann wird der Empfänger durch eine Fehlermeldung an den E-Mail-Client benachrichtigt, wenn er versucht, E-Mail abzuholen.

☞ Ist für die E-Mail-Client-Software die Option „Gelesene E-Mails auf dem Server löschen“ aktiviert, so wird bei der Einstellung „Benachrichtigung per E-Mail“ die infizierte Mail auf dem Server gelöscht, da der E-Mail-Client davon ausgeht, daß die E-Mail erfolgreich übertragen wurde. Ist dies nicht gewünscht (wenn z.B. die infizierte E-Mail auf anderem Weg heruntergeladen werden soll), sollte ausschließlich die Option „Fehlermeldung an den E-Mail Client“ genutzt werden.

bei Überschreiten der Grössenbegrenzung

E-Mail ungescannt durchlassen
Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlassmodus, wenn die eingestellte Dateigröße überschritten wird.

☞ In diesem Fall findet keine Überprüfung auf Viren statt!

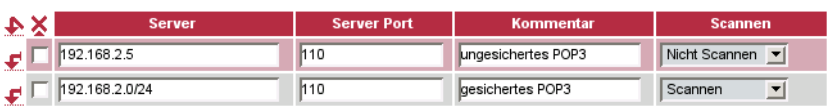
E-Mail blockieren
Diese Option bewirkt die Ausgabe eines Fehlercodes an den E-Mail-Client und das Blockieren der E-Mail.

Liste der POP3 Server

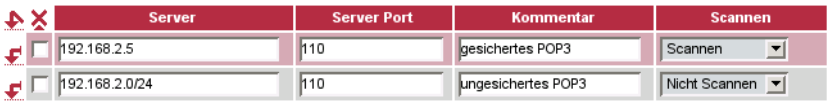
Sie können die Server auswählen, deren Datenverkehr gefiltert werden soll und für jede IP explizit angeben, ob der Antivirus-Schutz aktiviert werden soll oder nicht. Dadurch ist auch die Angabe von „trusted“ Servern möglich.

Beispiele:
Globale Aktivierung des Antivirus-Schutzes für POP3:

Scan eines Subnetzes, Ausklammerung eines „trusted“ POP3-Servers:



Scan eines einzelnen „untrusted“ POP3 Servers in einem Subnetz:



- Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also ausschlaggebend für das Ergebnis.
- Der Virenfilter kann parallel nur eine begrenzte Anzahl gleichzeitiger Verbindungen zu Mail-, HTTP- und FTP-Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.
- Das Einschalten des POP3 Virenfilters öffnet die Firewall für die entsprechenden Ports unabhängig von zusätzlichen anderslautenden Firewall-Regeln.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. der Datenverkehr aller POP3-Server wird gefiltert. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140.

- Da ein Verbindungswunsch zunächst durch den Proxy entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert, da der Proxy nur Anfragen an die in der Liste angegebenen Adressen entgegennimmt.

Server Port

Hier geben Sie bitte die Nummer des Ports für das POP3-Protokoll an. Der POP3-Standardport **110** ist bereits voreingestellt.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Scannen

Scannen

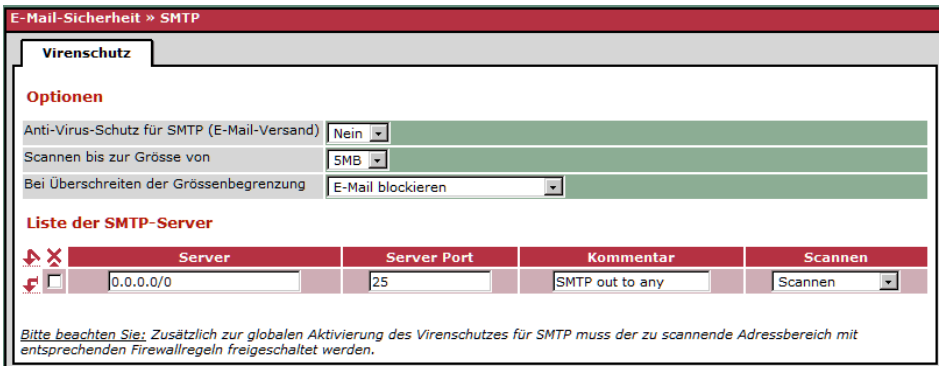
Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

6.8.2 E-Mail-Sicherheit →SMTP

Virenschutz



Das SMTP-Protokoll wird von Ihrem E-Mail-Client oder Mail-Transfer-Agent (MTA) zur Versendung von E-Mails genutzt.

- Der Virenfilter kann nur unverschlüsselte Daten auf Viren untersuchen. Deshalb sollten Sie Verschlüsselungsoptionen wie TLS nicht aktivieren. Im Falle des Erkennens eines Virus oder beim Auftreten von Fehlern wird der E-Mail-Client des Absenders durch einen Fehlercode benachrichtigt und ein Logeintrag im Antivirus-Log vorgenommen. Der ursprüngliche Empfänger erhält weder die infizierte Mail noch eine Benachrichtigung.
- Bei Aktivierung des Virenschutzes für SMTP-Mail-Versand muss unter "Liste der SMTP-Server" durch eine entsprechende Firewallregel der Adressbereich des/der entsprechenden SMTP-Server freigeschaltet werden.

Optionen

Anti-Virus-Schutz für SMTP (E-Mail-Versand): Ja / Nein

Bei **Ja** wird eine Port-Redirection für SMTP-Verbindungen auf den SMTP-Proxy angelegt.

Scannen bis zur Grösse von

Voreingestellt: 5 MB. Hier geben Sie die Maximalgröße der zu überprüfenden Dateien an.

Wird diese Grenze überschritten, wird abhängig von der Einstellung „bei Überschreitung der Grössenbegrenzung“ eine Fehlermeldung an den SMTP-Client zurückgegeben und die E-Mail nicht gesendet oder automatisch in den Durchlassmodus geschaltet.

Wenn die Speicherkapazität des mGuard nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an den E-Mail-Client des Benutzers ausgegeben und ein Eintrag im Antivirus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, das Versenden zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlassmodus aktivieren.

☞ Bitte beachten Sie, dass die Größe des Anhangs je nach Kodierung u.U. ein Vielfaches der ursprünglichen Dateigröße sein kann.

Bei Überschreiten der Grössenbegrenzung

E-Mail ungescannt durchlassen

Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlassmodus, wenn die eingestellte Dateigröße überschritten wird.

☞ In diesem Fall wird nicht auf Viren überprüft!

E-Mail blockieren

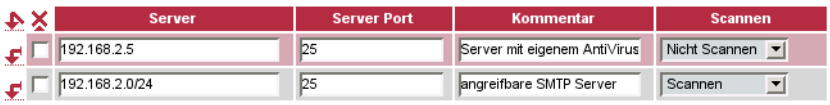
Diese Option bewirkt die Ausgabe eines Fehlercodes an den E-Mail-Client und das Blockieren der E-Mail.

Liste der SMTP Server

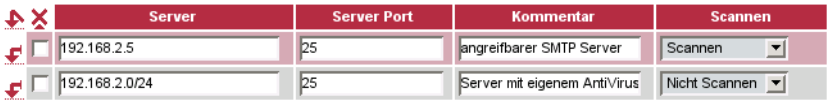
Sie können die Server angeben, zu denen Datenverkehr gefiltert werden soll und für jede IP explizit angeben, ob der Antivirus-Schutz aktiviert werden soll oder nicht.

Beispiele:
Globale Aktivierung des Antivirus-Schutzes für SMTP:

Scan eines Subnetzes, Ausklammerung eines SMTP-Servers:



Scan für einen einzelnen SMTP-Server in einem Subnetz:



- Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also ausschlaggebend für das Ergebnis.
- Der Virenfilter kann parallel nur eine begrenzte Anzahl gleichzeitiger Verbindungen zu Mail-, HTTP- und FTP-Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.
- Das Einschalten des SMTP Virenfilters öffnet die Firewall für die entsprechenden Ports unabhängig von zusätzlichen anderslautenden Firewall-Regeln.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. der Datenverkehr zu allen SMTP-Servern wird gefiltert. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140.

- Da ein Verbindungswunsch zunächst durch den Proxy entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert, da der Proxy nur Anfragen an die in der Liste angegebenen Adressen entgegennimmt.

Server Port

Hier geben Sie bitte die Nummer des Ports für das SMTP-Protokoll an. Der SMTP-Standardport **25** ist bereits voreingestellt.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Scannen

Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

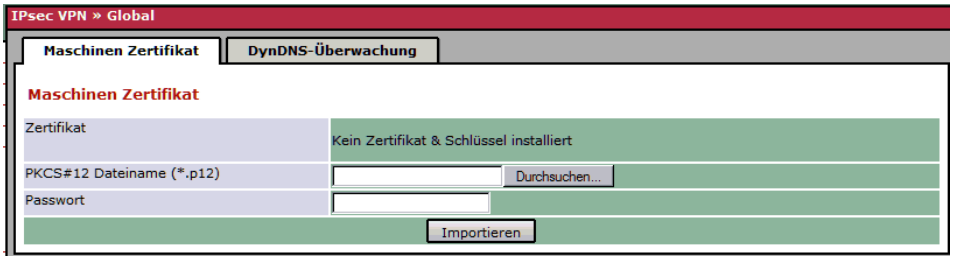
Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

6.9 Menü IPsec VPN (nicht blade Controller)

6.9.1 IPsec VPN → Global

Maschinen Zertifikat



Maschinen Zertifikat

Zeigt das aktuell importierte X.509-Zertifikat an, mit dem sich der mGuard gegenüber anderen VPN-Gateways ausweist. Folgende Informationen werden angezeigt:

subject	Der Besitzer, auf den das Zertifikat ausgestellt ist.
issuer	Die Beglaubigungsstelle, die das Zertifikat unterschrieben hat. C : Land (Country) ST: Bundesland (State) L : Stadt (Location) O : Organisation OU: Abteilung (Organisation Unit) CN: Hostname, allgemeiner Name (Common Name)
MD5, SHA1 Fingerprint	Fingerabdruck des Zertifikats, um diesen z. B. am Telefon mit einem anderen zu vergleichen. Windows zeigt an dieser Stelle den Fingerabdruck im SHA1-Format an.
notBefore, notAfter	Gültigkeitszeitraum des Zertifikats. Wird vom mGuard mangels einer eingebauten Uhr ignoriert.

Die importierte Zertifikatsdatei (Dateinamen-Erweiterung *.p12 oder *.pfx) enthält neben den oben angegebenen Informationen die beiden Schlüssel, den öffentlichen zum Verschlüsseln, den privaten zum Entschlüsseln. Der zugehörige öffentliche Schlüssel kann an beliebig viele Verbindungspartner vergeben werden, so dass diese verschlüsselte Daten senden können.
In Abhängigkeit von der Gegenstelle muss das Zertifikat als .cer- oder .pem-Datei dem Bediener der entfernten Gegenstelle zur Verfügung gestellt werden - z. B. durch persönliche Übergabe oder per E-Mail. Wenn Ihnen kein sicherer Übertragungsweg zur Verfügung steht, sollten Sie anschließend den vom mGuard angezeigten Fingerabdruck über einen sicheren Weg vergleichen.

Es kann nur eine Zertifikats-Datei (PKCS#12-Datei) ins Gerät importiert werden.
Um ein (neues) Zertifikat zu importieren, gehen Sie wie folgt vor:

Neues Zertifikat importieren

Voraussetzung:

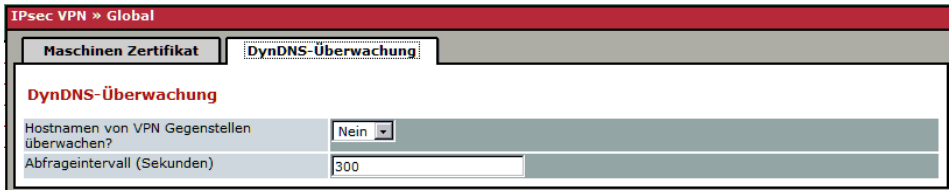
Die Zertifikatsdatei (Dateiname = *.p12 oder *.pfx) ist generiert und auf dem angeschlossenen Rechner gespeichert.

Hinter **PKCS#12 Dateiname (*.p12)**:

1. **Durchsuchen...** klicken, um die Datei zu selektieren
2. In das Feld *Passwort* geben Sie das Passwort ein, mit dem der private Schlüssel der PKCS#12-Datei geschützt ist.
3. **Importieren** klicken.

Nach dem Import ist unter *Zertifikat* das geladenene Zertifikat zu sehen.

DynDNS-Überwachung



Erläuterung zu DynDNS siehe unten: Dienste → DynDNS Registrierung.

DynDNS-Überwachung

Hostnamen von VPN Gegenstellen überwachen? Ja / Nein

Ist dem mGuard die Adresse einer VPN-Gegenstelle als Hostname angegeben (siehe „VPN-Verbindung definieren“ auf Seite 125), und ist dieser Hostname bei einem DynDNS Service registriert, dann kann der mGuard regelmäßig überprüfen, ob beim betreffenden DynDNS eine Änderung erfolgt ist. Falls ja, wird die VPN-Verbindung zu der neuen IP-Adresse aufgebaut.

Abfrageintervall (Sekunden)

Standard: 300 (Sekunden)

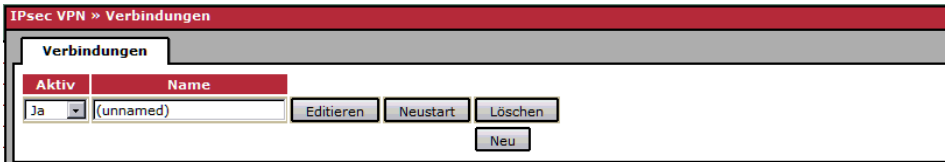
6.9.2 IPsec VPN → Verbindungen

Voraussetzungen für eine VPN-Verbindung:
Generelle Voraussetzung für eine VPN-Verbindung ist, dass die IP-Adressen der VPN-Partner bekannt und zugänglich sind.

- Damit eine IPsec-Verbindung erfolgreich aufgebaut werden kann, muss die VPN-Gegenstelle IPsec mit folgender Konfiguration unterstützen:
  – Authentifizierung über Pre-Shared Key (PSK) oder X.509 Zertifikate
  – ESP
  – Diffie-Hellman Gruppe 2 oder 5
  – DES, 3DES oder AES encryption
  – MD5 oder SHA-1 Hash Algorithmen
  – Tunnel oder Transport Modus
  – Quick Mode
  – Main Mode
  – SA Lifetime (1 Sekunde bis 24 Stunden)
  Ist die Gegenstelle ein Rechner unter Windows 2000, muss dazu das *Microsoft Windows 2000 High Encryption Pack* oder mindestens das *Service Pack 2* installiert sein.
- Befindet sich die Gegenstelle hinter einem NAT-Router, so muss die Gegenstelle NAT-T unterstützen. Oder aber der NAT-Router muss das IPsec-Protokoll kennen (IPsec/VPN Passthrough). In beiden Fällen sind aus technischen Gründen nur IPsec Tunnel-Verbindungen möglich.

Verbindungen

.



Hier werden alle definierten VPN-Verbindungen aufgelistet.

- **Definierte VPN-Verbindung aktivieren / deaktivieren**:
  Parameter **Aktiv** auf **Ja** bzw. **Nein** setzen.
- **Definierte VPN-Verbindung bearbeiten**:
  Neben dem Listeneintrag auf die Schaltfläche **Editieren** klicken.
- **Definierte VPN-Verbindung löschen**:
  Neben dem Listeneintrag auf die Schaltfläche **Löschen** klicken.
- **VPN-Verbindung neu starten**:
  Neben dem Listeneintrag auf die Schaltfläche **Neustart** klicken. Dann wird die bestehende Verbindung beenden und neu aufgebaut.
- **Neue VPN-Verbindung definieren**:
  1. auf die Schaltfläche **Neu** klicken.
     Folge: Die angezeigte Liste der VPN-Verbindungen erhält einen weiteren Eintrag.
  2. Neben diesem Listeneintrag die Schaltfläche **Editieren** klicken.

⌦ Zwecks Fernsteuerung können VPN Verbindungen auch unabhängig von der Einstellung **Aktiv** auch durch abfragen der folgenden URL aktiviert und deaktiviert werden:

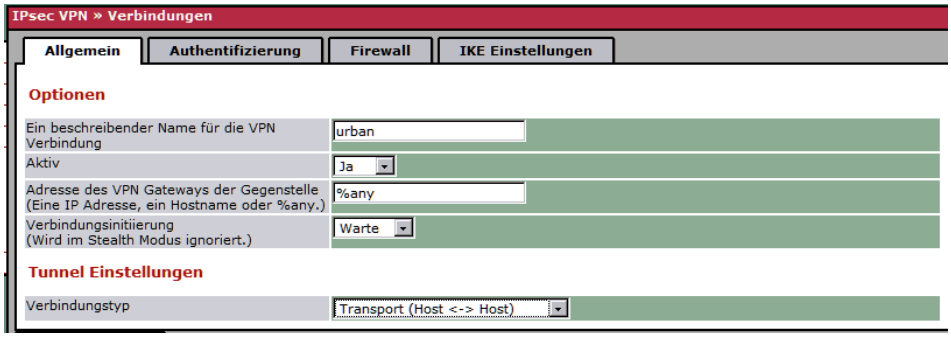
`https://`*login*`:`*passwort*`@`*host*`/nph-vpn.cgi?name=`*verbindung*`&cmd=(`up|down*)*

Beispiel:

6.9.3 VPN-Verbindung definieren

Nach Klicken auf **Editieren** erscheint folgende Seite

Allgemein:



Optionen

Ein beschreibender Name für die VPN Verbindung

Sie können die Verbindung frei benennen bzw. umbenennen.

Aktiv: Ja / Nein

Legen Sie fest, ob die Verbindung aktiv (= Ja) sein soll oder nicht (= Nein).

Adresse des VPN Gateways der Gegenstelle

(Eine IP-Adresse, ein Hostname oder %any)

Die Adresse des Übergangs zum privaten Netz, in dem sich der entfernte Kommunikationspartner befindet.

– Falls der mGuard aktiv die Verbindung zur entfernten Gegenstelle initiieren und aufbauen soll oder sich im *Stealth*-Modus befindet, dann geben Sie hier die IP-Adresse des Gegenstellen-Gateway an. Statt einer IP-Adresse können Sie auch einen Hostnamen (d. h. Domain Namen im URL-Format in der Form vpn.example.com) eingeben.
– Falls der VPN Gateway der Gegenstelle keine feste und bekannte IP-Adresse hat, kann über die Inanspruchname des DynDNS-Service (siehe Glossar) dennoch eine feste und bekannte Adresse simuliert werden.
– Falls der mGuard bereit sein soll, die Verbindung anzunehmen, die eine entfernte Gegenstelle mit beliebiger IP-Adresse aktiv zum lokalen mGuard initiiert und aufbaut, dann geben Sie an: **%any**
So kann eine entfernte Gegenstelle den lokalen mGuard „anrufen“, wenn diese Gegenstelle ihre eigene IP-Adresse (vom Internet Service Provider) dynamisch zugewiesen erhält, d. h. eine wechselnde IP-Adresse hat. Nur wenn in diesem Szenario die entfernte „anrufende“ Gegenstelle auch eine feste und bekannte IP-Adresse hat, können Sie diese IP-Adresse angeben.

⌧ **%any** kann nur zusammen mit dem Authentisierungsverfahren über X.509 Zertifikate verwendet werden.

⌧ Wenn sich die Gegenstelle hinter einem NAT Gateway befindet, muß **%any** gewählt werden. Ansonsten wird das Aushandeln weiterer Verbindungsschlüssel nach der ersten Kontaktaufnahme fehlschlagen.

Verbindungsinitiierung: Initiiere / Warte

Initiiere

In diesem Fall initiiert der lokale mGuard die Verbindung zur Gegenstelle. Im Feld *Adresse des VPN Gateways der Gegenstelle* (s. o.) muss die feste IP-Adresse der Gegenstelle oder deren Domain Name eingetragen sein.

Warte

In diesem Fall ist der lokale mGuard bereit, die Verbindung anzunehmen, die eine entfernte Gegenstelle aktiv zum lokalen mGuard initiiert und aufbaut.

☞ Wenn Sie unter *Adresse des VPN Gateways der Gegenstelle* **%any** eingetragen haben, müssen Sie **Warte** auswählen.

☞ Arbeitet der mGuard im *Stealth*-Modus, ist diese Einstellung wirkungslos. D. h. sie wird ignoriert und die Verbindung wird automatisch initiiert, wenn der mGuard bemerkt, dass die Verbindung genutzt werden soll.

Tunnel Einstellungen

Verbindungstyp

Es stehen zur Auswahl:

- Tunnel (Netz ←→ Netz)
- Transport (Host ←→ Host)
- Transport (L2TP Microsoft Windows)
- Transport (L2TP SSH Sentinel)

Tunnel (Netz ←→ Netz)

Dieser Verbindungstyp eignet sich in jedem Fall und ist der sicherste. In diesem Modus werden die zu übertragenen IP-Datagramme vollkommen verschlüsselt und mit einem neuen Header versehen zur VPN-Gateway der Gegenstelle, dem „Tunnelende“, gesendet. Dort werden die übertragenen Datagramme entschlüsselt und aus ihnen die ursprünglichen Datagramme wiederhergestellt. Diese werden dann zum Zielrechner weitergeleitet.

Transport (Host ←→ Host)

Bei diesem Verbindungstyp werden nur die Daten der IP-Pakete verschlüsselt. Die IP Header Informationen bleiben unverschlüsselt.

Transport (L2TP Microsoft Windows)
Transport (L2TP SSH Sentinel)

Ist beim entfernten Rechner der Verbindungstyp IPsec/L2TP aktiviert, dann setzen Sie den mGuard auch auf *Transport (L2TP Microsoft Windows)* für ältere Microsoft Windows Versionen bzw. *Transport (SSH Sentinel)* für den SSH Sentinel Client oder neuere Microsoft Windows Versionen oder Service Packs.
Innerhalb der IPsec-Transport-Verbindung schafft das L2TP/PPP Protokoll einen Tunnel. Dem extern angeschlossenen IPsec/L2TP-Rechner wird seine IP-Adresse vom mGuard dynamisch zugewiesen.
Aktivieren Sie dazu auch den L2TP-Server des mGuards.

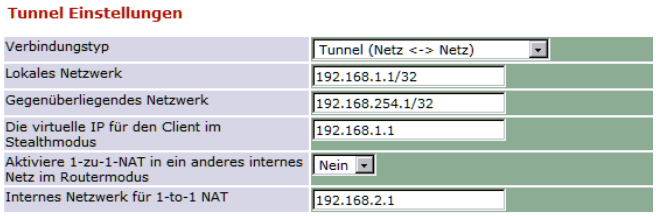
☞ Bei Verwendung eines Microsoft Windows Clients setzen Sie *Perfect Forward Secrecy (PFS)* auf **Nein** (siehe unten).

☞ Sobald unter Windows die IPsec/L2TP-Verbindung gestartet wird,

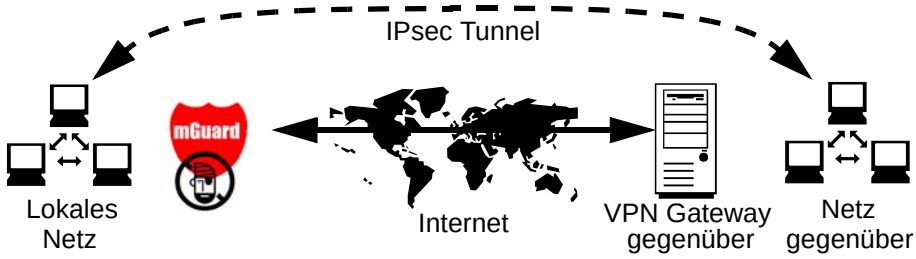
erscheint ein Dialogfeld, das nach Benutzername und Login fragt. Sie können dort beliebige Einträge machen, denn die Authentifizierung erfolgt bereits über die X.509 Zertifikate, so dass der mGuard diese Eingaben ignoriert.

Tunnel Einstellungen, bei Verbindungstyp Tunnel (Netz ←→ Netz)

Ist der *Verbindungstyp* auf „Tunnel (Netz ←→Netz)“ gesetzt, erscheinen weitere Einstellmöglichkeiten auf der Seite.



Machen Sie dort folgende Angaben:



Lokales Netzwerk

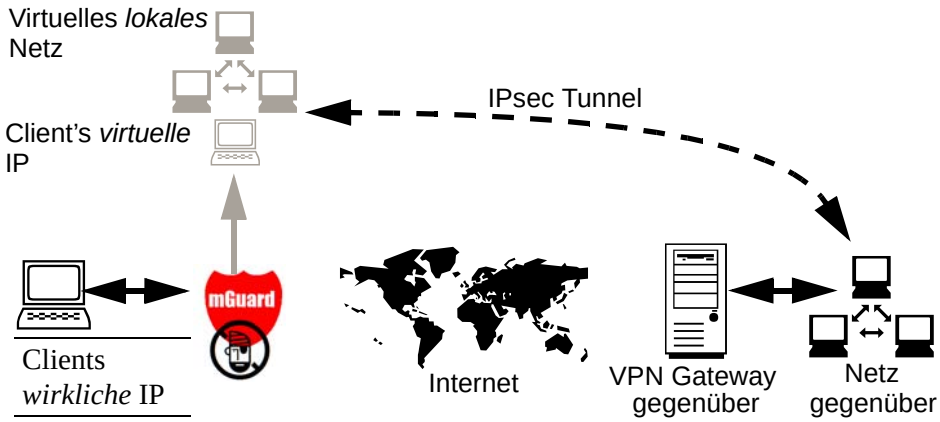
Hier geben Sie die Adresse des Netzes oder Computers an, das/der lokal am mGuard angeschlossen ist.

Gegenüberliegendes Netzwerk

Hier geben Sie die Adresse des Netzes oder Computers an, das/der sich hinter dem gegenüberliegenden VPN Gateway befindet.

☞ Die Adresse 0.0.0.0/0 gibt eine *Default Route über das VPN* an.
Bei dieser wird sämtlicher Datenverkehr, für den keine anderen Tunnel oder Routen existieren, durch diesen VPN Tunnel geleitet.
Eine Default Route über das VPN sollte nur für einen Tunnel angegeben werden.
Im *Stealth* Modus kann eine *Default Route über das VPN* nicht verwendet werden.

Die virtuelle IP für den Client im Stealth Modus



Im *Stealth*-Modus wird das lokale Netz des VPNs durch den mGuard simuliert. Innerhalb dieses *virtuellen* Netzes ist der Client unter einer *virtuellen* IP bekannt.

⌦ Dieser Eintrag wird nur im *Stealth*-Modus benötigt.

Aktiviere 1-zu-1-NAT in ein anderes internes Netz im Router-Modus: Ja / Nein

Das im VPN Tunnel angegebene lokale Netzwerk auf ein am lokalen (LAN) Ethernetport vorhandenes lokales Netzwerk umschreiben.

Eine Erläuterung zu 1-zu-1-NAT finden Sie unter „Netzwerksicherheit → NAT“, „1:1-NAT“ auf Seite 103

Internes Netzwerk für 1-zu-1-NAT

Die Netzwerkaddresse am lokalen (LAN) Ethernetport. Die Netzmaske wird aus dem Feld *Lokales Netzwerk* übernommen.

Authentifizierung

Authentication

Authentisierungsverfahren

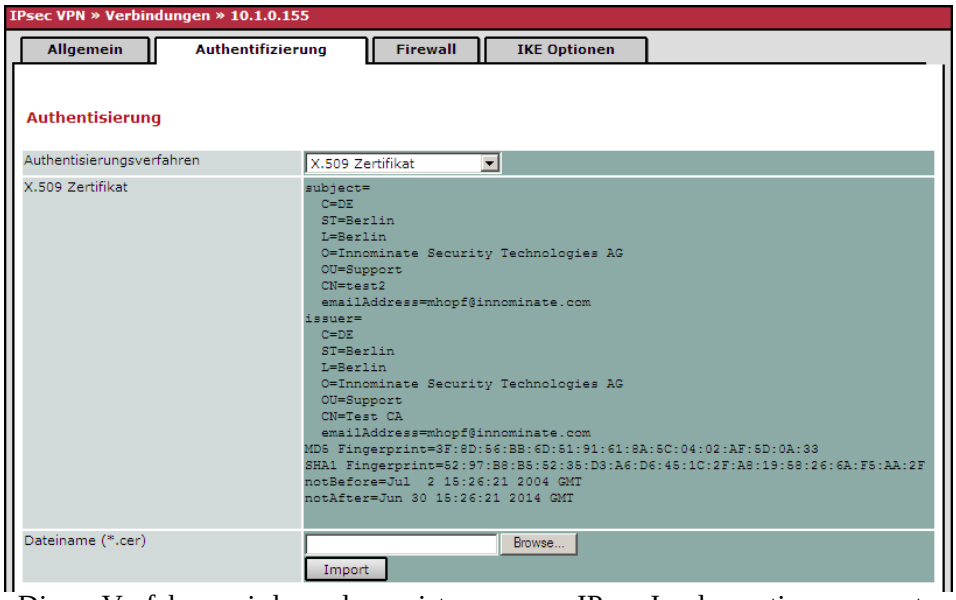
Es gibt 2 Möglichkeiten:

– X.509 Zertifikat

– Pre-Shared Key

Je nach dem, welches Sie auswählen, zeigt die Seite unterschiedliche Einstellmöglichkeiten.

Authentisierungsverfahren: Bei Authentisierungsverfahren X.509 Zertifikat



Dieses Verfahren wird von den meisten neueren IPsec-Implementierungen unterstützt. Dabei verschlüsselt der mGuard die Authentifizierungs-Datagramme, die es zur Gegenstelle, dem „Tunnelende“ sendet, mit dem öffentlichen Schlüssel (Dateiname *.cer oder *.pem) der Gegenstelle. (Diese *.cer- oder *.pem-Datei haben Sie vom Bediener der Gegenstelle erhalten, z. B. per Diskette oder per E-Mail).

Um diesen öffentlichen Schlüssel dem mGuard zur Verfügung zu stellen, gehen Sie wie folgt vor:

Voraussetzung:

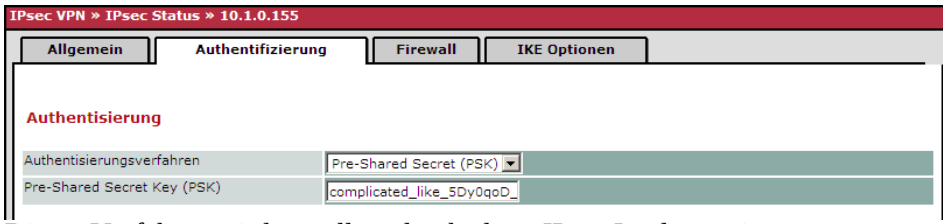
Sie haben die *.cer- oder *.pem-Datei auf dem Rechner gespeichert.

1. **Durchsuchen...** klicken und die Datei selektieren.
2. **Importieren** klicken.

   Nach dem Import wird der Inhalt des neuen Zertifikats angezeigt. Eine Erläuterung der angezeigten Informationen finden Sie im Abschnitt „IPsec VPN → Global“ auf Seite 122.

Nachdem ein X.509 Zertifikat importiert worden ist, wird das geladene Zertifikat angezeigt.

Authentisierungsverfahren: Bei Authentisierungsverfahren Pre-Shared Secret (PSK)



Dieses Verfahren wird vor allem durch ältere IPsec Implementierungen unterstützt. Dabei authentifizieren sich beide Seiten des VPNs über den gleichen PSK.

Um den verabredeten Schlüssel dem mGuard zur Verfügung zu stellen, gehen Sie wie folgt vor:

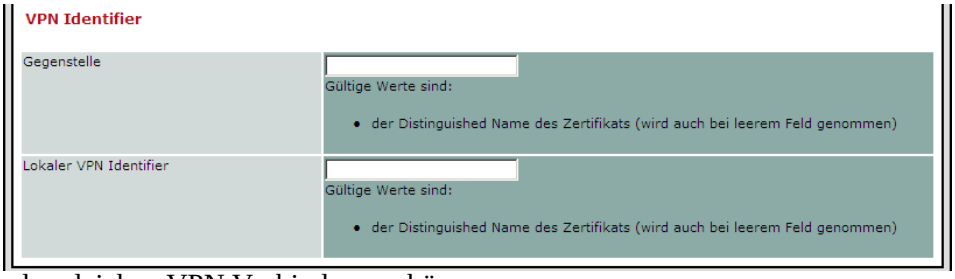
Ins Eingabefeld *Pre-Shared Secret Key (PSK)* die verabredete Zeichenfolge eintragen.

Um eine mit 3DES vergleichbare Sicherheit zu erzielen, sollte die Zeichenfolge aus ca. 30 nach dem Zufallsprinzip ausgewählten Klein- und Großbuchstaben sowie Ziffern bestehen.

☞ *Pre-Shared Secret Key* kann nicht mit dynamischen (%any) IP-Adressen verwendet werden, nur feste IP-Adressen oder Hostnamen auf beiden Seiten werden unterstützt.

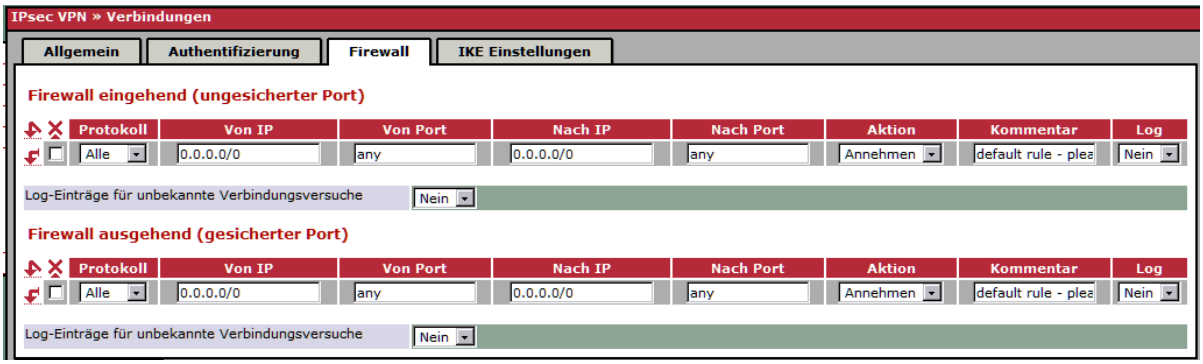
VPN Identifier

Über *VPN Identifier* erkennen die VPN Gateways, welche Konfigurationen zu


VPN Identifier
Gegenstelle
Gültige Werte sind:
der Distinguished Name des Zertifikats (wird auch bei leerem Feld genommen)
Lokaler VPN Identifier
Gültige Werte sind:
der Distinguished Name des Zertifikats (wird auch bei leerem Feld genommen)

der gleichen VPN Verbindung gehören.
Sind diese Felder leer, so wird im Falle von X.509 Zertifikaten der *Distinguished Name* des Zertifikats verwendet oder aber im Falle von PSK die IP Adressen der VPN Gateways.

Firewall



Firewall eingehend (ungesicherter Port), Firewall ausgehend (gesicherter Port)

Während die unter dem Menüpunkt *Netzwerk Sicherheit* vorgenommenen Einstellungen sich nur auf Nicht-VPN-Verbindungen beziehen (siehe oben unter „Menü Netzwerksicherheit (nicht blade Controller)“ auf Seite 98), beziehen sich die Einstellungen hier ausschließlich auf die VPN-Verbindung, die auf diesem Registerkarten-Set definiert ist. Das bedeutet praktisch: Haben Sie mehrere VPN-Verbindungen definiert, können Sie für jede einzelne den Zugriff von außen oder von innen beschränken. Versuche, die Beschränkungen zu übergehen, können Sie ins Log protokollieren lassen.

⌦ Gemäß werksseitiger Voreinstellung ist die VPN-Firewall so eingestellt, dass für diese VPN-Verbindung alles zugelassen ist.
Für jede einzelne VPN-Verbindung gelten aber unabhängig voneinander gleichwohl die erweiterten Firewall-Einstellungen, die weiter oben definiert und erläutert sind - siehe „Menü Netzwerksicherheit (nicht blade Controller)“, „Netzwerksicherheit → Packet Filter“, „Erweiterte Einstellungen“ auf Seite 101.

⌦ Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der

Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

⌦ Im *Stealth*-Modus ist in den Firewallregeln die vom Client wirklich verwendete IP-Adresse zu verwenden oder aber auf 0.0.0.0/0 zu belassen, da nur ein Client durch den Tunnel angesprochen werden kann.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

Von IP/Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 140.

Bei aktiviertem 1-zu-1-NAT ist hier als Ziel-IP-Adresse für eingehende Verbindungen sowie als Quell-IP-Adresse für ausgehende Verbindungen jeweils die echte IP-Adresse im 1-zu-1-NAT-Netz anzugeben.

Von Port/Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen (s. u.).)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

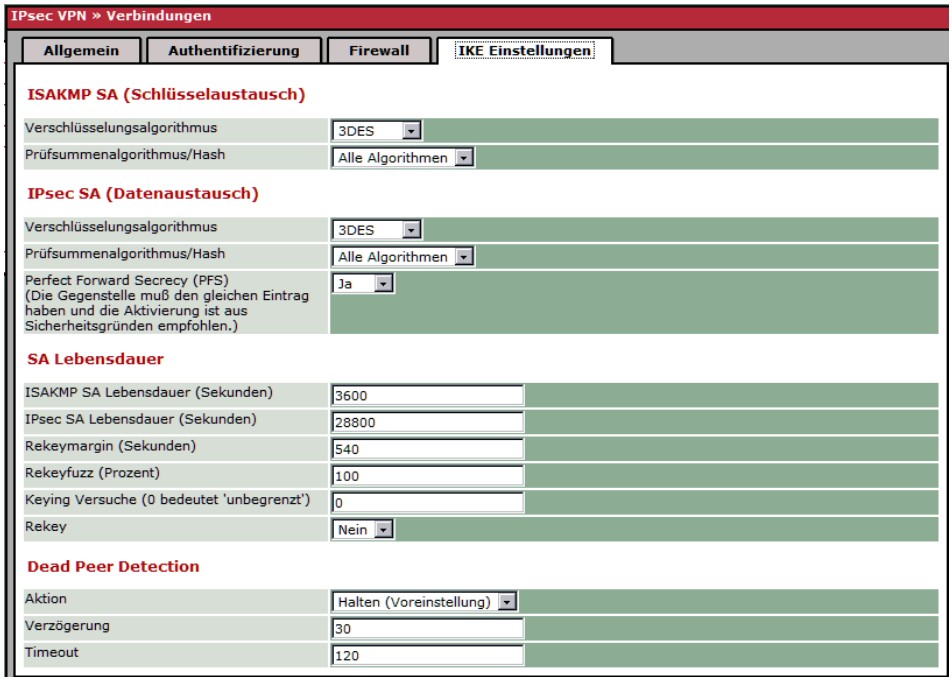
Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche

Bei **Ja** werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

IKE Optionen



ISAKMP SA (Schlüsselaustausch)

Verschlüsselungsalgorithmus

☞ Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verschlüsselungsverfahren verwendet werden soll.

3DES-168 ist das am häufigsten benutzte Verfahren und ist deshalb als Standard voreingestellt.

Grundsätzlich gilt Folgendes: Je mehr Bits ein Verschlüsselungsalgorithmus hat - angegeben durch die angefügte Zahl -, desto sicherer ist er. Das relativ neue Verfahren AES-256 gilt daher als am sichersten, ist aber noch nicht so verbreitet.

Der Verschlüsselungsvorgang ist um so zeitaufwendiger, je länger der Schlüssel ist. Dieser Gesichtspunkt spielt für den mGuard keine Rolle, weil er mit Hardware-basierter Verschlüsselungstechnik arbeitet. Jedoch könnte dieser Aspekt für die Gegenstelle eine Rolle spielen.

Der zur Auswahl stehende mit „Null“ bezeichnete Algorithmus beinhaltet keinerlei Verschlüsselung.

Prüfsummenalgorithmus/Hash

Lassen Sie die Einstellung auf *Alle Algorithmen* stehen. Dann spielt es keine Rolle, ob die Gegenstelle mit MD5 oder SHA-1 arbeitet.

IPsec SA (Datenaustausch)

Im Unterschied zu *ISAKMP SA (Schlüsselaustausch)* (s. o.) wird hier das Verfahren für den Datenaustausch festgelegt. Die können sich von denen des Schlüsselaustauschs unterscheiden, müssen aber nicht.

Verschlüsselungsalgorithmus

Siehe oben.

Prüfsummenalgorithmus/Hash

Siehe oben.

Perfect Forward Secrecy (PFS)

Verfahren zur zusätzlichen Steigerung der Sicherheit bei der Datenübertragung. Bei IPsec werden in bestimmten Intervallen die Schlüssel für den Datenaustausch erneuert. Mit PFS werden dabei mit der Gegenstelle neue Zufallszahlen ausgehandelt, anstatt sie aus zuvor verabredeten Zufallszahlen abzuleiten.

☞ Nur wenn die Gegenstelle PFS unterstützt, wählen Sie **Ja**.

☞ Bei Auswahl des Verbindungstyps *Transport (L2TP Microsoft Windows)* setzen Sie *Perfect Forward Secrecy (PFS)* auf **Nein**.

SA Lebensdauer

Die Schlüssel einer IPsec Verbindung werden in bestimmten Abständen erneuert, um die Kosten eines Angriffs auf eine IPsec Verbindung zu erhöhen.

ISAKMP SA Lebensdauer (Sekunden)

Lebensdauer der für die ISAKMP SA vereinbarten Schlüssel in Sekunden. Die Werkseinstellung sind 3600 Sekunden (1 Stunde). Das erlaubte Maximum sind 86400 Sekunden (24 Stunden).

IPsec SA Lebensdauer (Sekunden)

Lebensdauer der für die IPsec SA vereinbarten Schlüssel in Sekunden.

Die Werkseinstellung sind 28800 Sekunden (8 Stunden). Das erlaubte Maximum sind 86400 Sekunden (24 Stunden).

Rekey Margin (Sekunden)

Minimale Zeitspanne vor Ablauf der alten Schlüssel, innerhalb der ein neuer Schlüssel erzeugt werden soll. Werkseinstellung: 540 Sekunden (9 Minuten).

Rekeyfuzz (Prozent)

Maximum in Prozent, um das *Rekey Margin* zufällig vergrößert werden soll. Dies dient dazu, den Schlüsselaustausch auf Maschinen mit vielen VPN-Verbindungen zeitversetzt stattfinden zu lassen. Werkseinstellung: 100 Prozent.

Keying Versuche

Anzahl der Versuche, die unternommen werden sollen, neue Schlüssel mit der Gegenstelle zu vereinbaren.

Der Wert 0 bedeutet bei Verbindungen, die der mGuard initiieren soll, unendlich viele Versuche, ansonsten 5 Versuche.

Rekey

Bei **Ja** wird der mGuard versuchen, einen neuen Schlüssel zu vereinbaren, wenn die Gültigkeit des alten abläuft.

Dead Peer Detection

Wenn die Gegenstelle das Dead Peer Detection (DPD) Protokoll unterstützt, können die jeweiligen Partner erkennen, ob die IPsec Verbindung noch gültig ist oder nicht und evtl. neu aufgebaut werden muss.

Ohne DPD muß je nach Konfiguration bis zum Ablauf der SA Lebensdauer gewartet werden oder die Verbindung manuell neu initiiert werden.

Aktion

Bei **Halten** (Voreinstellung) wird versucht, die IPsec Verbindung neu aufzubauen, wenn diese für tot erklärt wurde, aber nur, wenn das lokal angeschlossene Netz versucht, Daten zur Gegenstelle zu senden.

Bei **Löschen** wird nicht versucht die Verbindung erneut aufzubauen.

Die Werkseinstellung ist **Hold**.

Verzögerung

Zeitspanne in Sekunden, nach welcher *DPD Keep Alive* Anfragen gesendet werden sollen. Diese Anfragen testen ob die Gegenstelle noch verfügbar ist. Werkseinstellung: 30 Sekunden.

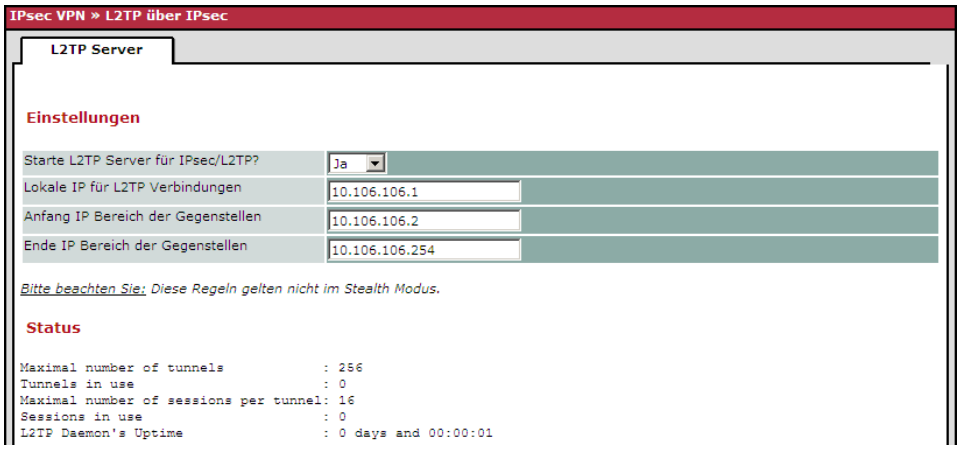
Timeout

Zeitspanne in Sekunden, nach der die Verbindung zur Gegenstelle für tot erklärt werden soll, wenn auf die *Keep Alive* Anfragen keine Antwort erfolgte. Werkseinstellung: 120 Sekunden.

6.9.4 IPsec VPN → L2TP über IPsec

Zusammen mit VPN Verbindungen vom Verbindungstyp Transport ermöglicht der L2TP Server, dass Gegenstellen über IPsec/L2TP mit dem mGuard ein VPN aufbauen können.

L2TP Server


IPsec VPN » L2TP über IPsec
L2TP Server
Einstellungen
Starte L2TP Server für IPsec/L2TP?
Ja
Lokale IP für L2TP Verbindungen
10.106.106.1
Anfang IP Bereich der Gegenstellen
10.106.106.2
Ende IP Bereich der Gegenstellen
10.106.106.254
Bitte beachten Sie: Diese Regeln gelten nicht im Stealth Modus.
Status
Maximal number of tunnels : 256
Tunnels in use : 0
Maximal number of sessions per tunnel: 16
Sessions in use : 0
L2TP Daemon's Uptime : 0 days and 00:00:01

Einstellungen

Starte L2TP Server für IPsec/L2TP? Ja / Nein

Wollen Sie IPsec/L2TP-Verbindungen ermöglichen, setzen Sie diesen Schalter auf **Ja**.

Über IPsec können dann zum mGuard L2TP Verbindungen aufgebaut werden, über welche den Clients dynamisch IP Adressen innerhalb des VPNs zugeteilt werden.

Lokale IP für L2TP Verbindungen

Nach dem obigen Screenshot teilt der mGuard der Gegenstelle mit, er habe die Adresse 10.106.106.1.

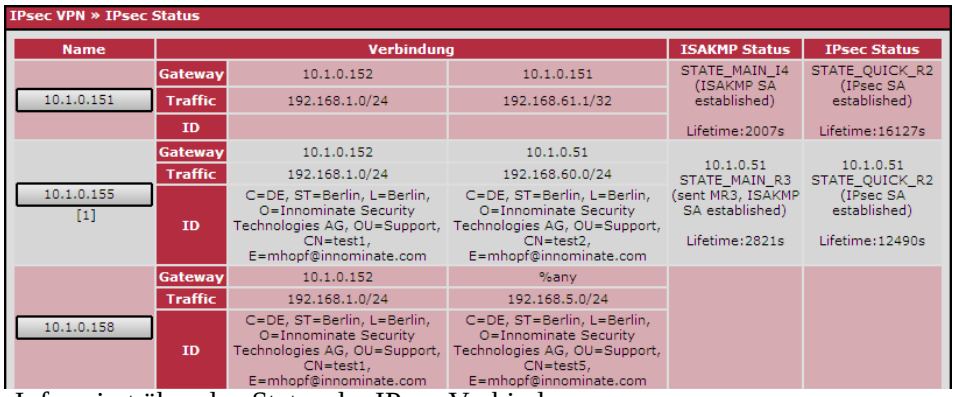
Anfang / Ende IP Bereich der Gegenstellen

Nach dem obigen Screenshot teilt der mGuard der Gegenstelle eine IP Adresse zwischen 10.106.106.2 und 10.106.106.254 mit.

Status

Informiert über den L2TP-Status, wenn dieser als Verbindungstyp gewählt ist.

6.9.5 IPsec VPN → IPsec Status



Informiert über den Status der IPsec-Verbindungen.
Links sind die Namen der VPN-Verbindungen aufgelistet, rechts daneben wird jeweils deren aktueller Status angezeigt.

GATEWAY
: zeigt die IP Adressen der miteinander kommunizierenden VPN Gateways

TRAFFIC
: bezeichnet Rechner bzw. Netze, die über die VPN-Gateways kommunizieren.

ID
: bezeichnet den Distinguished Name (DN) eines X.509-Zertifikats.

ISAKMP Status
: *ISAKMP Status* (Internet security association and key management protocol) ist mit „established“ angegeben, wenn die beiden beteiligten VPN-Gateways einen Kanal zum Schlüsselaustausch aufgebaut haben. In diesem Fall konnten sie einander kontaktieren, und alle Einträge bis einschließlich „ISAKMP SA“ auf der Konfigurationsseite der Verbindung waren korrekt.

IPsec Status
: *IPsec Status* ist mit „established“ angegeben, wenn die IPsec-Verschlüsselung bei der Kommunikation aktiviert ist. In diesem Fall waren auch die Angaben unter „IPsec SA“ und „Tunnel-Einstellungen“ korrekt.

Bei Problemen empfiehlt es sich, in die VPN-Logs des Rechners zu schauen, zu dem die Verbindung aufgebaut wurde. Denn der initiierende Rechner bekommt aus Sicherheitsgründen keine ausführlichen Fehlermeldungen zugesandt.

Falls angezeigt wird:
: *ISAKMP SA established, IPsec State: WAITING*

Dann bedeutet das:
Die Authentifizierung war erfolgreich, jedoch stimmten die anderen Parameter nicht: Stimmt der Verbindungstyp (Tunnel, Transport) überein? Wenn Tunnel gewählt ist, stimmen die Netzbereiche auf beiden Seiten überein?

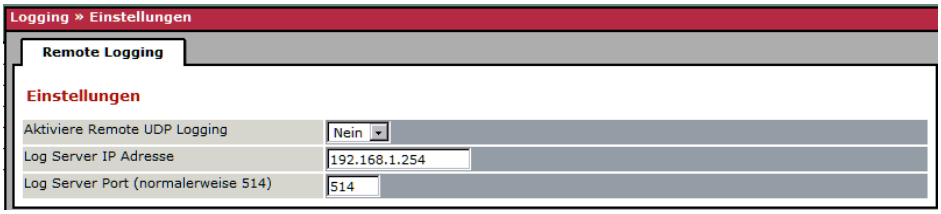
Falls angezeigt wird:
: *IPsec State: IPsec SA established*

Dann bedeutet das:
Die VPN-Verbindung ist erfolgreich aufgebaut und kann genutzt werden. Sollte dies dennoch nicht der Fall sein, dann gibt es Probleme mit dem VPN-Gateway der Gegenstelle. In diesem Fall die Verbindung deaktivieren und wieder aktivieren, um die Verbindung erneut aufzubauen.

6.10 Menü Logging

6.10.1 Logging → Einstellungen

Remote Logging



Alle Log-Einträge finden standardmäßig im Arbeitsspeicher des mGuard statt. Ist der maximale Speicherplatz für diese Protokollierungen erschöpft, werden automatisch die ältesten Log-Einträge durch neue überschrieben. Zudem werden bei Ausschalten des mGuard alle Log-Einträge gelöscht.
Um das zu verhindern, ist es möglich, die Log-Einträge auf einen externen Rechner zu übertragen. Das liegt auch dann nahe, sollte eine zentrale Verwaltung der Protokollierungen erfolgen.

Einstellungen

Aktiviere remote UDP Logging: Ja / Nein

Sollen alle Log-Einträge zum externen (unten angegebenen) Log Server übertragen werden, setzen Sie diesen Schalter auf **Ja**.

Log Server IP Adresse

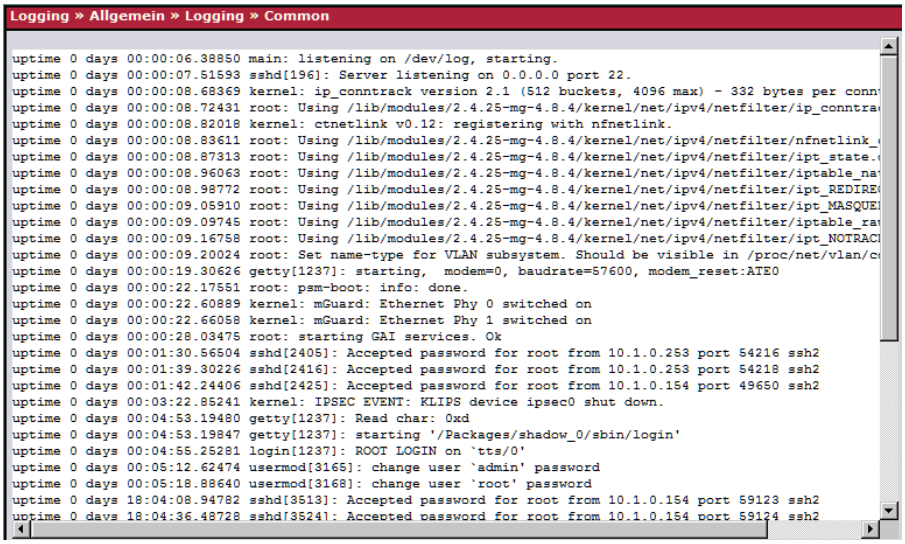
Geben Sie die IP-Adresse des Log Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen.

☞ Sie müssen eine IP-Adresse angeben, keinen Hostnamen! Hier wird eine Namensauflösung nicht unterstützt, weil sonst der Ausfall eines DNS-Servers nicht protokolliert werden könnte.

Log Server Port (normalerweise 514)

Geben Sie den Port des Log Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen. Standard: 514

6.10.2 Logging → Logs ansehen


Logging » Allgemein » Logging » Common
uptime 0 days 00:00:06.38850 main: listening on /dev/log, starting.
uptime 0 days 00:00:07.51593 sshd[196]: Server listening on 0.0.0.0 port 22.
uptime 0 days 00:00:08.68369 kernel: ip_conntrack version 2.1 (512 buckets, 4096 max) - 332 bytes per conn
uptime 0 days 00:00:08.72431 root: Using /lib/modules/2.4.25-mg-4.8.4/kernel/net/ipv4/netfilter/ip_conntra
uptime 0 days 00:00:08.82018 kernel: ctnetlink v0.12: registering with nfnetlink.
uptime 0 days 00:00:08.83611 root: Using /lib/modules/2.4.25-mg-4.8.4/kernel/net/ipv4/netfilter/nfnetlink_
uptime 0 days 00:00:08.87313 root: Using /lib/modules/2.4.25-mg-4.8.4/kernel/net/ipv4/netfilter/ipt_state.
uptime 0 days 00:00:08.96063 root: Using /lib/modules/2.4.25-mg-4.8.4/kernel/net/ipv4/netfilter/iptable_na
uptime 0 days 00:00:08.98772 root: Using /lib/modules/2.4.25-mg-4.8.4/kernel/net/ipv4/netfilter/ipt_REDIRE
uptime 0 days 00:00:09.05910 root: Using /lib/modules/2.4.25-mg-4.8.4/kernel/net/ipv4/netfilter/ipt_MASQUE
uptime 0 days 00:00:09.09745 root: Using /lib/modules/2.4.25-mg-4.8.4/kernel/net/ipv4/netfilter/iptable_ra
uptime 0 days 00:00:09.16758 root: Using /lib/modules/2.4.25-mg-4.8.4/kernel/net/ipv4/netfilter/ipt_NOTRAC
uptime 0 days 00:00:09.20024 root: Set name-type for VLAN subsystem. Should be visible in /proc/net/vlan/c
uptime 0 days 00:00:19.30626 getty[1237]: starting, modem=0, baudrate=57600, modem_reset:ATE0
uptime 0 days 00:00:22.17551 root: psm-boot: info: done.
uptime 0 days 00:00:22.60889 kernel: mGuard: Ethernet Phy 0 switched on
uptime 0 days 00:00:22.66058 kernel: mGuard: Ethernet Phy 1 switched on
uptime 0 days 00:00:28.03475 root: starting GAI services. Ok
uptime 0 days 00:01:30.56504 sshd[2405]: Accepted password for root from 10.1.0.253 port 54216 ssh2
uptime 0 days 00:01:39.30226 sshd[2416]: Accepted password for root from 10.1.0.253 port 54218 ssh2
uptime 0 days 00:01:42.24406 sshd[2425]: Accepted password for root from 10.1.0.154 port 49650 ssh2
uptime 0 days 00:03:22.85241 kernel: IPSEC EVENT: KLIPS device ipsec0 shut down.
uptime 0 days 00:04:53.19480 getty[1237]: Read char: 0xd
uptime 0 days 00:04:53.19847 getty[1237]: starting '/Packages/shadow_0/sbin/login'
uptime 0 days 00:04:55.25281 login[1237]: ROOT LOGIN on `tts/0'
uptime 0 days 00:05:12.62474 usermod[3165]: change user `admin' password
uptime 0 days 00:05:18.88640 usermod[3168]: change user `root' password
uptime 0 days 18:04:08.94782 sshd[3513]: Accepted password for root from 10.1.0.154 port 59123 ssh2
uptime 0 days 18:04:36.48728 sshd[3524]: Accepted password for root from 10.1.0.154 port 59124 ssh2

Zeigt Logeinträge der ausgewählter Kategorien an.

Netzwerksicherheit

Ist bei Festlegung von Firewall-Regeln das Protokollieren von Ereignissen festgelegt (Log = Ja), dann können Sie hier das Log aller protokollierten Ereignisse einsehen.

AntiVirus

Das Virus-Log enthält folgende Meldungen des Virenfilters:

- Gefundene Viren mit Angabe von Details (Name des Virus, Name der Datei, bei einer E-Mail zusätzlich: Absender, Datum, Betreff)
- Ausgegebene Warnungen bei automatischer Einschaltung des Durchlassmodus, wenn die zu filternde Datei die eingestellte Dateigröße überschreitet und nicht gefiltert wurde.
- Start und Fehlerausgaben des Virenfilters

Fehlermeldungen

Virus Detection

Ein Virus wurde erkannt. Die Fehlermeldung umfasst den Namen des Virus, den Absender der E-Mail, das Absendedatum und den Namen der infizierten Datei bzw. den Namen der komprimierten Archivdatei und des infizierten Bestandteils dieses Archivs.

Beispiel einer Virenmeldung:

```
mGuard detected a virus. The mail could not be delivered.
found Virus Email-Worm.Win32.NetSky.q /[From
sick@example.com][Date Fri, 13 Aug 2004 11:33:53++0200]/
about_you.zip/document.txt.exe
[000012a7.00000077.00000000]
Message Details:
From: sick@example.com
Subject: Private document
Date: Fri, 13 Aug 2004 11:33:53 +0200
```

Exceeded maximum filesize

Die eingestellte Begrenzung der Dateigröße wurde überschritten.

Um die Datei trotzdem übertragen zu können, deaktivieren Sie für den Download den Virenfilter für den entsprechenden Server oder global. Alternativ können Sie

den Durchlassmodus (Menüpunkt: „bei Überschreiten der Größenbegrenzung) im jeweiligen Protokoll aktivieren.

⌦ In beiden Fällen wird die übertragene Datei nicht nach Viren untersucht!

Temporary Virus Scanner Failure
Ein temporärer Fehler trat bei dem Versuch auf, eine Datei zu scannen. Eine Wiederholung der Übertragung zu einem späteren Zeitpunkt oder ein Update der Virensignaturdatei kann evtl. das Problem beheben.
Mögliche Fehlerursachen:

- Die Scan-Engine ist nicht in der Lage, die Datei zu bearbeiten
- Die Speicherkapazität des Innominate mGuard reicht nicht zur Dekompression der Datei aus
- Interner Fehler der Scan-Engine

Exceptional Virus Scanner Failure
Ein Kommunikationproblem mit der Scan-Engine trat auf.
Mögliche Fehlerursachen:

- Fehlgeschlagenes Signatur-Update durch fehlerhafte Angabe des Update-Servers (Menüpunkt Antivirus->Database Update)
- Ungültige Lizenz für den Virenfilter
- Beschädigtes oder fehlerhaftes Update der Virensignaturdatei

Update running
Der Virenfilter verfügt über keine Virensignaturen, der Download der Virensignaturen wurde bereits gestartet. Sie können den Fortschritt des Downloads im Menüpunkt Logging-> AntiVirus Update verfolgen.

AntiVirus Update

Das Update-Log enthält Meldungen über den Start und Verlauf des Update-Prozesses der Virensignaturdateien.

IPsec VPN

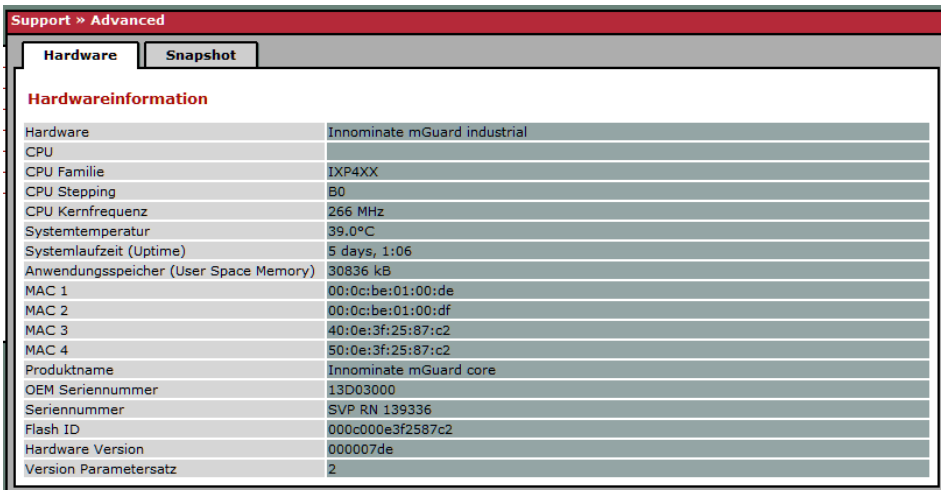
Listet alle VPN-Ereignisse auf.
Das Format entspricht dem unter Linux gebräuchlichen Format.
Es gibt spezielle Auswertungsprogramme, die Ihnen die Informationen aus den protokollierten Daten in einem besser lesbaren Format präsentieren.

6.11 Menü Support

6.11.1 Support → Erweitert

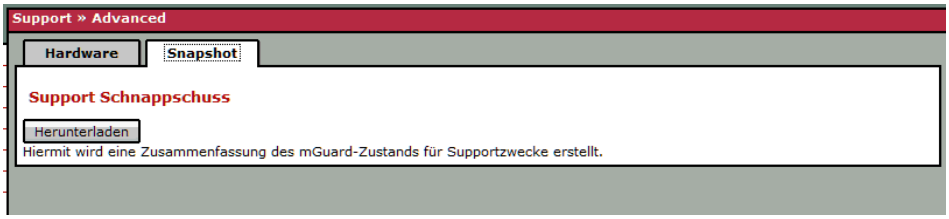
Hardware

Nur Anzeige



Diese Seite listet verschiedene Hardwareeigenschaften des mGuards auf.

Snapshot



Diese Funktion dient für Support-Zwecke.
Erstellt eine komprimierte Datei (im tar-Format), in der alle aktuellen Konfigurations-Einstellungen und Log-Einträge erfasst sind, die zur Fehlerdiagnose relevant sein könnten.

⌧ Diese Datei einthält keine privaten Informationen wie z. B. das private Maschinen-Zertifikat oder Passwörter. Eventuell benutzte Pre-Shared Keys von VPN-Verbindungen sind jedoch in Snapshots enthalten.

Um einen Snapshot zu erstellen, gehen Sie wie folgt vor:
1. Die Schaltfläche **Herunterladen** klicken.
2. Die Datei speichern (unter dem Namen snapshot.tar.gz)

Stellen Sie die Datei dem Support zur Verfügung, wenn dies erforderlich ist.

6.12 CIDR (Classless InterDomain Routing)

IP Netzmasken und CIDR sind Notationen, die mehrere IP-Adressen zu einem Adressraum zusammenfassen. Dabei wird ein Bereich von aufeinanander folgenden Adressen als ein Netzwerk behandelt.

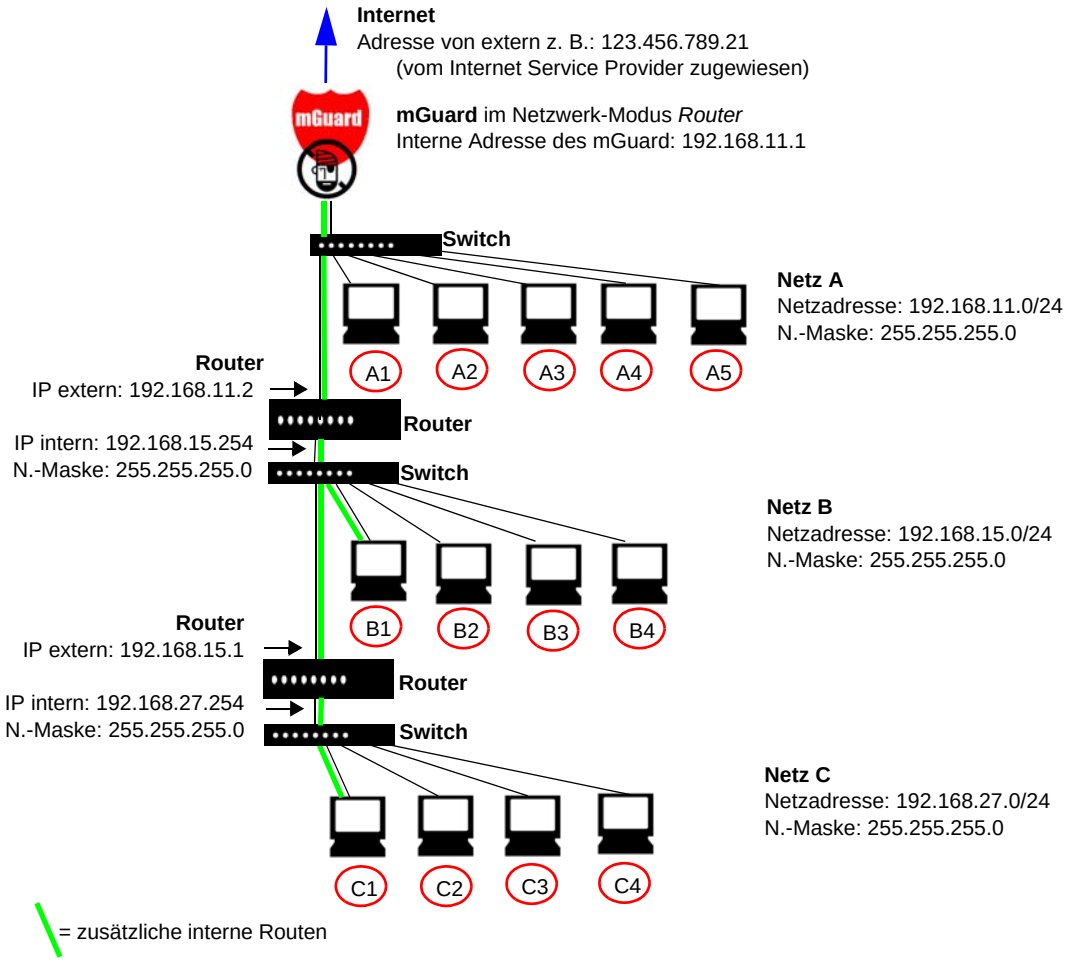
Um dem mGuard einen Bereich von IP-Adressen anzugeben, z. B. bei der Konfiguration der Firewall, kann es erforderlich sein, den Adressraum in der CIDR-Schreibweise anzugeben. Die nachfolgende Tabelle zeigt links die IP-Netzmaske, ganz rechts die entsprechende CIDR-Schreibweise.

IP-Netzmaske	binär				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

Beispiel: 192.168.1.0 / 255.255.255.0 entspricht im CIDR: 192.168.1.0/24

6.13 Netzwerk-Beispielskizze

Die nachfolgende Skizze zeigt, wie in einem lokalen Netzwerk mit Subnetzen die IP-Adressen verteilt sein könnten, welche Netzwerk-Adressen daraus resultieren und wie die Angabe einer zusätzlichen internen Route lauten könnte.



Netz A

Rechner	A1	A2	A3	A4	A5
IP-Adresse	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Netz B

Rechner	B1	B2	B3	B4
IP-Adresse	192.168.15.2	192.168.15.3	192.168.15.4	192.168.15.5
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Netz C

Rechner	C1	C2	C3	C4
IP-Adresse	192.168.27.1	192.168.27.2	192.168.27.3	192.168.27.4
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Zusätzliche interne Routen:

Netzwerk: 192.168.15.0/24
Gateway: 192.168.11.2

Netzwerk: 192.168.27.0/24
Gateway: 192.168.11.2

7 Die Rescue-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware

Die Rescue-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

7.1 Neustart durchführen

Ziel Das Gerät neu starten mit den konfigurierten Einstellungen.

Aktion: **Rescue-Taste** für ca. 1,5 Sekunden drücken:
- blade, PCI: bis beide roten LEDs aufleuchten
- delta: bis die Status LED aufhört zu blinken
- industrial: bis die Status LED und die Link-LEDs aufhören zu leuchten
- smart: Bis die mittlere LED in Rot aufleuchtet.

ODER
- Die Stromzufuhr vorübergehend unterbrechen.
- mGuard PCI: Den Computer, welcher die mGuard PCI Karte enthält, neu starten.

7.2 Recovery-Prozedur ausführen

Ziel Auf den mGuard kann nicht mehr zugegriffen werden und die Netzwerkkonfiguration soll in den Auslieferungszustand zurückgesetzt werden: Der Stealthmodus mit der Adresse 1.1.1.1 und beim mGuard delta und bei der mGuard blade Control Unit der Routermodus mit der Adresse 192.168.1.1.

Weiterhin wird für die Ethernetanschlüsse das MAU Management eingeschaltet, HTTPS über den lokalen Ethernetanschluß (LAN) freigegeben

⌦ Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:
Der mGuard befindet sich im Router- oder PPPoE-Modus und
– die Geräteadresse des mGuard ist konfiguriert worden abweichend von der Standardeinstellung und
– Sie kennen die aktuelle IP-Adresse des Gerätes nicht.

Aktion:

1. Die **Rescue-Taste** langsam 6-mal drücken.
2. Nach ca. 2 Sekunden antwortet der mGuard:

- blade, PCI
  - Bei Erfolg leuchtet die LAN LED rot
  - Bei Mißerfolg leuchtet die WAN LED rot
- delta
  - Bei Erfolg leuchtet die Status LED grün
  - Bei Mißerfolg bleibt die Status LED aus.
- industrial
  - Bei Erfolg leuchtet die STATUS LED gelb
  - Bei Mißerfolg leuchtet die ERROR LED rot
- smart
  - Bei Erfolg leuchtet die mittlere LED grün
  - Bei Mißerfolg leuchtet die mittlere LED rot

3. Drücken Sie anschließend erneut die **Resuce-Taste** langsam 6-mal.
4. Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den *Stealth*-Modus (mGuard delta: Router-Modus). Es ist dann wieder unter folgender Adresse zu erreichen:**https://1.1.1.1/** (mGuard delta und mGuard blade Control Unit: 192.168.1.1)

7.3 Flashen der Firmware

Ziel Die gesamte Software des mGuard soll neu ins Gerät geladen werden.

⌧ **Alle konfigurierten Einstellungen werden gelöscht.** Der mGuard wird in den Auslieferungszustand versetzt.

Mögliche Gründe zum Flashen der Firmware:

- Das Administrator- und Root-Passwort sind verloren gegangen.

Aktion: Gehen Sie wie folgt vor:

⌧ **Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des mGuard unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.**

Voraussetzungen:

- Sie haben die Software des mGuard von der mGuard-CD kopiert oder vom Innominate-Support bezogen und auf dem Konfigurations-Rechner gespeichert.
- DHCP- und TFTP-Server sind auf einem gemeinsamen Rechner installiert - siehe „Voraussetzungen zum Flashen der Firmware: DHCP- und TFTP-Server” auf Seite 145.
- mGuard PCI: Wird der mGuard im Power-over-PCI Modus betrieben, muss der DHCP/TFTP Server über die LAN Buchse des mGuard angeschlossen sein.
  Wird der mGuard im PCI Treibermodus betrieben, muss der DHCP/TFTP Server unter dem Rechner bzw. Betriebssystem ausgeführt werden, das die Schnittstelle zum mGuard bereitstellt.

1. **Rescue-Taste** gedrückt halten, bis der *Recovery-Status* wie folgt eintritt:

   Der mGuard wird neu gestartet (nach ca. 1,5 Sekunden), nach weiteren ca. 1,5 Sekunden gelangt der mGuard in den *Recovery-Status*:
   - blade, PCI: die grünen sowie die rote LAN LED leuchten
   - delta: die Status LED wird langsam dunkel
   - industrial: die LEDs 1, 2 und V.24 leuchten
   - smart: alle LEDs leuchten grün.

2. Spätestens 1 Sekunde nach Eintritt des *Recovery-Status* die **Rescue-Taste** loslassen. (Falls Sie die **Rescue-Taste** nicht loslassen, wird der mGuard neu gestartet.)
   Der mGuard startet nun das Recovery-System: Er sucht über die Schnittstelle für den lokal angeschlossenen Rechner bzw. für das lokal angeschlossene Netzwerk nach dem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

- Statusanzeige:
  - blade, PCI: die rote LAN LED blinkt
  - delta: die Status LED blinkt
  - industrial: die LEDs 1, 2 und V.24 leuchten orange auf
  - smart: die mittlere LED (Heartbeat) blinkt

  Vom TFTP-Server wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur von Innominate unterschriebene Dateien werden geladen.
  Die Kontrollprozedur löscht nun den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Software vor.
- Statusanzeige:
  - blade, PCI: die grünen und die rote LAN LED bilden ein Lauflicht
  - delta: die Status LED blinkt schneller
  - industrial: die LEDs 1, 2 und V.24 bilden ein Lauflicht
  - smart: die 3 grünen LEDs bilden ein Lauflicht

  Vom TFTP-Server wird die Software jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Innominate signierte Dateien werden akzeptiert.
  Dieser Vorgang dauert ca. 3 bis 5 Minuten.
- Statusanzeige:
  - blade, PCI: blinken die grünen LEDs und die rote LAN LED gleichzeitig durchgehend
  - delta: die Status LED leuchtet kontinuierlich
  - industrial: die LEDs 1, 2 und V.24 sind aus, die LEDs p1, p2 und Status leuchten kontinuierlich grün
  - smart: Die mittlere LED (Heartbeart) leuchtet kontinuierlich.

  Die neue Software wird entpackt und konfiguriert. Das dauert ca. 5 Minuten.
  Sobald die Prozedur beendet ist
  - blade, PCI: startet sich der mGuard neu
  - delta: blinkt die Status LED einmal pro Sekunde
  - industrial: blinken die LEDs 1, 2 und V.24 gleichzeitig durchgehend grün
  - smart: blinken alle 3 LEDs gleichzeitig durchgehend grün

3. Starten Sie den mGuard neu. (nicht nötig bei blade und PCI)

Drücken Sie dazu kurz die **Rescue-Taste**.
ODER
Unterbrechen Sie seine Stromversorgung und schließen Sie ihn dann wieder an (smart: per USB-Kabel, das ausschließlich zur Stromversorgung dient) bzw. mGuard PCI starten Sie Ihren Computer neu.

Folge:
Der mGuard befindet sich im Auslieferungs-Zustand. Konfigurieren Sie ihn neu - siehe „Lokale Konfigurationsverbindung herstellen” auf Seite 42.

Voraussetzungen zum Flashen der Firmware: DHCP- und TFTP-Server

Zum „Flashen“ der Firmware muss auf dem lokal angeschlossenen Rechner bzw. Netzwerk-Rechner ein DHCP- und TFTP-Server installiert sein.
(DHCP = **D**ynamic **H**ost **C**onfiguration **P**rotocol; TFTP = **T**rivial **F**ile **T**ransfer **P**rotocol)

Installieren Sie den DHCP- und TFTP-Server, falls notwendig (siehe unten).

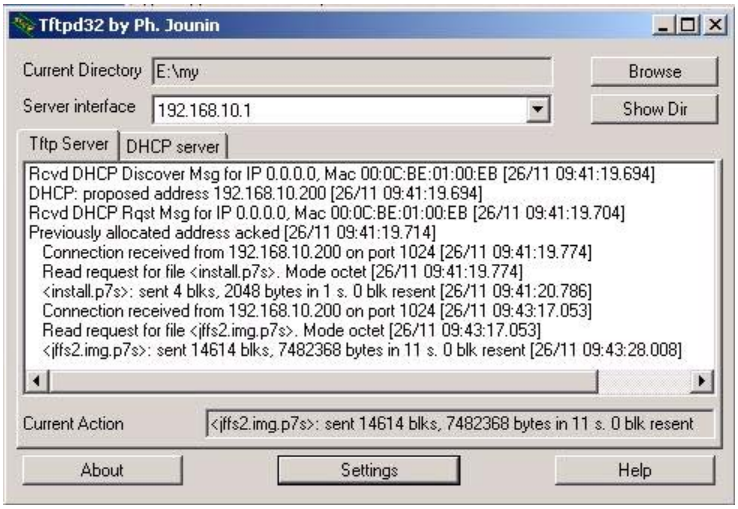
⌧ Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden!

DHCP- und TFTP-Server unter Windows installieren

Installieren Sie das Programm, das sich auf der CD befindet. Gehen Sie dazu wie folgt vor:

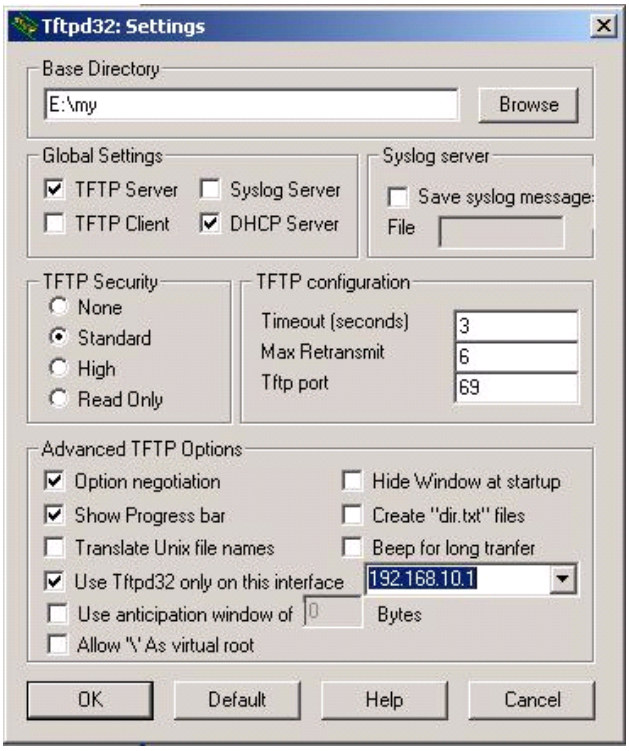
1. Ist der Windows-Rechner an einem Netzwerk angeschlossen, trennen Sie ihn von diesem.
2. Kopieren Sie die Software in einen beliebigen leeren Ordner des Windows-Rechners. Starten Sie das Programm TFTPD32.EXE
3. Die festzulegende Host-IP lautet: **192.168.10.1.** Das muss auch die Adresse für die Netzwerkkarte sein.
   Klicken Sie die Schaltfläche **Browse**, um auf den Ordner zu wechseln, wo die mGuard-Imagedateien gespeichert sind: *install.p7s*, *jffs2.img.p7s*

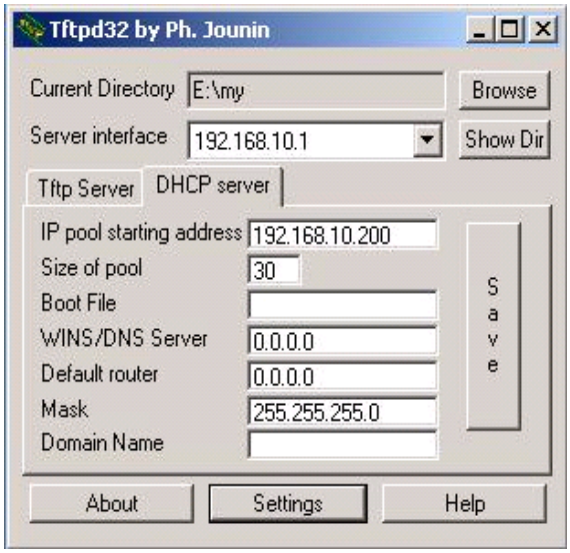
Die Image-Dateien befinden sich auch auf der CD, die zum Lieferumfang gehört.


Tftpd32 by Ph. Jounin
Current Directory E:\my
Browse
Server interface 192.168.10.1
Show Dir
Tftp Server
DHCP server
Rcvd DHCP Discover Msg for IP 0.0.0.0, Mac 00:0C:BE:01:00:EB [26/11 09:41:19.694]
DHCP: proposed address 192.168.10.200 [26/11 09:41:19.694]
Rcvd DHCP Rqst Msg for IP 0.0.0.0, Mac 00:0C:BE:01:00:EB [26/11 09:41:19.704]
Previously allocated address acked [26/11 09:41:19.714]
Connection received from 192.168.10.200 on port 1024 [26/11 09:41:19.774]
Read request for file <install.p7s>. Mode octet [26/11 09:41:19.774]
<install.p7s>: sent 4 blks, 2048 bytes in 1 s. 0 blk resent [26/11 09:41:20.786]
Connection received from 192.168.10.200 on port 1024 [26/11 09:43:17.053]
Read request for file <jffs2.img.p7s>. Mode octet [26/11 09:43:17.053]
<jffs2.img.p7s>: sent 14614 blks, 7482368 bytes in 11 s. 0 blk resent [26/11 09:43:28.008]
Current Action
<jffs2.img.p7s>: sent 14614 blks, 7482368 bytes in 11 s. 0 blk resent
About
Settings
Help

4. Wechseln Sie auf die Registerkarte *Tftp Server* bzw. *DHCP Server* und klicken Sie dann die Schaltfläche **Settings**, um im dann angezeigten Dialogfeld

die Parameter wie folgt zu setzen:





DHCP- und TFTP-Server unter Linux installieren

Alle aktuellen Linux-Distributionen enthalten DHCP- und TFTP-Server. Installieren Sie die entsprechenden Pakete gemäß der Anleitung der jeweiligen Distribution.
Konfigurieren Sie den DHCP-Server, indem Sie in der Datei **/etc/dhcp** folgende Einstellungen vornehmen:

```
subnet 192.168.134.0 netmask 255.255.255.0 {
range 192.168.134.100 192.168.134.119;
option routers 192.168.134.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.134.255;}
```

Diese Beispiel-Konfiguration stellt 20 IP-Adressen (.100 bis .119) bereit. Es wird angenommen, dass der DHCP-Server die Adresse 192.168.134.1 hat (Einstellungen für ISC DHCP 2.0).

Der benötigte TFTP-Server wird in folgender Datei konfiguriert:
/etc/inetd.conf
Fügen Sie in diese Datei die entsprechende Zeile ein oder setzen Sie die notwendigen Parameter für den TFTP-Service. (Verzeichnis für Daten ist: **/tftpboot)**

```
tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/
```

Starten Sie dann den inetd-Prozess neu, um die Konfigurationsänderungen zu übernehmen.
Sollten Sie einen anderen Mechanismus verwenden, z. B. xinetd, dann informieren Sie sich bitte in der entsprechenden Dokumentation.

8 Glossar

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung werden Daten mit einem Schlüssel verschlüsselt und mit einem zweiten Schlüssel wieder entschlüsselt. Beide Schlüssel eignen sich zum Ver- und Entschlüsseln. Einer der Schlüssel wird von seinem Eigentümer geheim gehalten (Privater Schlüssel/Private Key), der andere wird der Öffentlichkeit (Öffentlicher Schlüssel/Public Key), d. h. möglichen Kommunikationspartnern, gegeben.
Eine mit dem öffentlichen Schlüssel verschlüsselte Nachricht kann nur von dem Empfänger entschlüsselt und gelesen werden, der den zugehörigen privaten Schlüssel hat. Eine mit dem privaten Schlüssel verschlüsselte Nachricht kann von jedem Empfänger entschlüsselt werden, der den zugehörigen öffentlichen Schlüssel hat. Die Verschlüsselung mit dem privaten Schlüssel zeigt, daß die Nachricht tatsächlich vom Eigentümer des zugehörigen öffentlichen Schlüssels stammt. Daher spricht man auch von digitaler Signatur, Unterschrift.
Assymetrische Verschlüsselungsverfahren wie RSA sind jedoch langsam und anfällig für bestimmte Angriffe, weshalb sie oft mit einem symmetrischen Verfahren kombiniert werden (→ symmetrische Verschlüsselung). Andererseits sind Konzepte möglich, die die aufwendige Administrierbarkeit von symmetrischen Schlüsseln vermeiden.

DES / 3DES

Der von IBM stammende und von der NSA überprüfte symmetrische Verschlüsselungsalgorithmus (→ symmetrische Verschlüsselung) DES wurde 1977 vom amerikanischen National Bureau of Standards, dem Vorgänger des heutigen National Institute of Standards and Technology (NIST), als Standard für amerikanische Regierungsinstitutionen festgelegt. Das es sich hierbei um den ersten standardisierten Verschlüsslungsalgorithmus überhaupt handelte, setzte er sich auch schnell in der Industrie und somit außerhalb Amerikas durch.
DES arbeitet mit einer Schlüssellänge von 56Bit, die heute aufgrund der seit 1977 gestiegenen Rechenleistung der Computer als nicht mehr sicher gilt.
3DES ist eine Variante von DES. Es arbeitet mit 3 mal größeren Schlüsseln, die also 168 Bit lang sind. Sie gilt heute noch als sicher und ist unter anderem auch Teil des IPsec-Standards.

AES

Das NIST (National Institute of Standards and Technology) entwickelt in Zusammenarbeit mit Industrie-Unternehmen seit Jahren den AES-Verschlüsselungsstandard. Diese → symmetrische Verschlüsselung soll den bisherigen DES-Standard ablösen. Der AES-Standard spezifiziert drei verschiedene Schlüsselgrößen mit 128, 192 und 256 Bit.
1997 hatte die NIST die Initiative zu AES gestartet und ihre Bedingungen für den Algorithmus bekannt gegeben. Von den vorgeschlagenen Verschlüsselungsalgorithmen hat die NIST fünf Algorithmen in die engere Wahl gezogen; und zwar die Algorithmen MARS, RC6, Rijndael, Serpent und Twofish. Im Oktober 2000 hat man sich für Rijndael als Verschlüsselungsalgorithmus entschieden.

Client / Server

In einer Client-Server-Umgebung ist ein Server ein Programm oder Rechner, das vom Client-Programm oder Client-Rechner Anfragen entgegennimmt und beantwortet.
Bei Datenkommunikation bezeichnet man auch den Rechner als Client, der eine Verbindung zu einem Server (oder Host) herstellt. D. h. der Client ist der anrufende Rechner, der Server (oder Host) der angerufene.

Datagramm

Bei IP Übertragungsprotokollen werden Daten in Form von Datenpaketen, den sog. IP-Datagrammen, versendet. Ein IP-Datagramm hat folgenden Aufbau:

IP-Header	TCP, UDP, ESP etc. Header	Daten (Payload)

Der IP-Header enthält:
– die IP-Adresse des Absenders (source IP-address)
– die IP-Adresse des Empfängers (destination IP-adress)
– die Protokollnummer des Protokoll der nächst höheren Protokollschicht (nach dem OSI-Schichtenmodell)
– die IP-Header Prüfsumme (Checksum) zur Überprüfung der Integrität des Headers beim Empfang.

Der TCP-/UDP-Header enthält folgende Informationen:
– Port des Absenders (source port)
– Port des Empfängers (destination port)
– eine Prüfsume über den TCP-Header und ein paar Informationen aus dem IP-Header (u. a. Quell- und Ziel-IP-Adresse)

Default Route

Ist ein Rechner an ein Netzwerk angeschlossen, erstellt das Betriebssystem intern eine Routing-Tabelle. Darin sind die IP-Adressen aufgelistet, die das Betriebssystem von den angeschlossenen Rechnern und den gerade verfügbaren Verbindungen (Routen) ermittelt hat. Die Routing-Tabelle enthält also die mögliche Routen (Ziele) für den Versandt von IP-Paketen. Sind IP-Pakete zu verschicken, vergleicht das Betriebssystem des Rechners die in den IP-Paketen angegebenen IP-Adressen mit den Einträgen in der Routing-Tabelle, um die richtige Route zu ermitteln.
Ist ein Router am Rechner angeschlossen und ist dessen interne IP-Adresse als Standardgateway dem Betriebssystem mitgeteilt (bei der TCP//IP-Konfiguration der Netzwerkkarte), wird dessen IP-Adresse als Ziel verwendet, wenn alle anderen IP-Adressen der Routing-Tabelle nicht passen. In diesem Fall bezeichnet die IP-Adresse des Routers die Default Route, weil alle IP-Pakete (per Default = standardmäßig) zu diesem Gateway geleitet werden, deren IP-Adressen in der Routing-Tabelle sonst keine Entsprechnung, d. h. keine Route finden.

DynDNS-Anbieter

Auch *Dynamic DNS-Anbieter*. Jeder Rechner, der mit dem Internet verbunden ist, hat eine IP-Adresse (IP = Internet Protocol) Eine IP-Adresse besteht aus 4 maximal dreistelligen Nummern, jeweils durch einem Punkt getrennt. Ist der Rechner über die Telefonleitung per Modem, per ISDN oder auch per ADSL online, wird ihm vom Internet Service Provider dynamisch eine IP-Adresse zugeordnet, d. h. die Adresse wechselt von Sitzung zu Sitzung. Auch wenn der Rechner (z. B. bei einer Flatrate) über 24 Stunden ununterbrochen online ist, wird die IP-Adresse zwischendurch gewechselt.
Soll ein lokaler Rechner über das Internet erreichbar sein, muss er eine Adresse haben, die der entfernten Gegenstelle bekannt sein muss. Nur so kann diese die Verbindung zum lokalen Rechner aufbauen. Wenn die Adresse des lokalen Rechners aber ständig wechselt, ist das nicht möglich. Es sei denn, der Betreiber des lokalen Rechners hat ein Account bei einem DynamicDNS-Anbieter (DNS = Domain Name Server).
Dann kann er bei diesem einen Hostnamen festlegen, unter dem der Rechner künftig erreichbar sein soll, z. B.: www.example.com. Zudem stellt der DynamicDNS-Anbieter ein kleines Programm zur Verfügung, das auf dem betreffenden Rechner installiert und ausgeführt werden muss. Bei jeder Internet-Sitzung des lokalen Rechners teilt dieses Tool dem DynamicDNS-Anbieter mit, welche IP-Adresse der Rechner zurzeit hat. Dessen Domain Name Server registriert die

aktuelle Zuordnung Hostname - IP-Adresse und teilt diese anderen Domain Name Servern im Internet mit.
Wenn jetzt ein entfernte Rechner eine Verbindung herstellen will zum lokalen Rechner, der beim DynamicDNS-Anbieter registriert ist, benutzt der entfernte Rechner den Hostnamen des lokalen Rechners als Adresse. Dadurch wird eine Verbindung hergestellt zum zuständigen DNS (Domain Name Server), um dort die IP-Adresse nachzuschlagen, die diesem Hostnamen zurzeit zugeordnet ist. Die IP-Adresse wird zurückübertragen zum entfernten Rechner und jetzt von diesem als Zieladresse benutzt. Diese führt jetzt genau zum gewünschten lokalen Rechner.
Allen Internetadressen liegt im Grunde dieses Verfahren zu Grunde: Zunächst wird eine Verbindung zum DNS hergestellt, um die diesem Hostnamen zugeteilte IP-Adresse zu ermitteln. Ist das geschehen, wird mit dieser „nachgeschlagenen“ IP-Adresse die Verbindung zur gewünschten Gegenstelle, eine beliebige Internetpräsenz, aufgebaut.

IP-Adresse

Jeder Host oder Router im Internet / Intranet hat eine eindeutige IP-Adresse (IP = Internet Protocol). Die IP-Adresse ist 32 Bit (= 4 Byte) lang und wird geschrieben als 4 Zahlen (jeweils im Bereich 0 bis 255), die durch einen Punkt voneinander getrennt sind.
Eine IP-Adresse besteht aus 2 Teilen: die Netzwerk-Adresse und die Host-Adresse.

Netzwerk-Adresse	Host-Adresse

Alle Hosts eines Netzes haben dieselbe Netzwerk-Adresse, aber unterschiedliche Host-Adressen. Je nach Größe des jeweiligen Netzes - man unterscheidet Netze der Kategorie Class A, B und C - sind die beiden Adressanteile unterschiedlich groß:

	1. Byte	**2. Byte**	**3. Byte**	**4. Byte**
Class A	Netz-Adr.	Host-Adr.		
Class B	Netz-Adr.		Host-Adr.	
Class C	Netz-Adr.			Host-Adr.

Ob eine IP-Adresse ein Gerät in einem Netz der Kategorie Class A, B oder C bezeichnet, ist am ersten Byte der IP-Adresse erkennbar. Folgendes ist festgelegt:

	Wert des 1. Byte	**Bytes für die Netzadresse**	**Bytes für die Host-Adresse**
Class A	1 - 126	1	3
Class B	128 - 191	2	2
Class C	192 - 223	3	1

Rein rechnerisch kann es nur maximal 126 Class A Netze auf der Welt geben, jedes dieser Netze kann maximal 256 x 256 x 256 Hosts umfassen (3 Bytes Adressraum). Class B Netze können 64 x 256 mal vorkommen und können jeweils bis zu 65.536 Hosts enthalten (2 Bytes Adressraum: 256 x 256). Class C Netze können 32 x 256 x 256 mal vorkommen und können jeweils bis zu 256

Hosts enthalten (1 Byte Adressraum).

Subnetz-Maske
Einem Unternehmens-Netzwerk mit Zugang zum Internet wird normalerweise nur eine einzige IP-Adresse offiziell zugeteilt, z. B. 123.456.789.21. Bei dieser Beispiel-Adresse ist am 1. Byte erkennbar, dass es sich bei diesem Unternehmens-Netzwerk um ein Class B Netz handelt, d. h. die letzten 2 Byte können frei zur Host-Adressierung verwendet werden. Das ergibt rein rechnerisch einen Adressraum von 65.536 möglichen Hosts (256 x 256).
Ein so riesiges Netz macht wenig Sinn. Hier entsteht der Bedarf, Subnetze zu bilden. Dazu dient die Subnetz-Maske. Diese ist wie eine IP-Adresse ein 4 Byte langes Feld. Den Bytes, die die Netz-Adresse repräsentieren, ist jeweils der Wert 255 zugewiesen. Das dient vor allem dazu, sich aus dem Host-Adressenbereich einen Teil zu „borgen“, um diesen zur Adressierung von Subnetzen zu benutzen. So kann beim Class B Netz (2 Byte für Netzwerk-Adresse, 2 Byte für Host-Adresse) mit Hilfe der Subnetz-Maske 255.255.255.0 das 3. Byte, das eigentlich für Host-Adressierung vorgesehen war, jetzt für Subnetz-Adressierung verwendet werden. Rein rechnerisch können so 256 Subnetze mit jeweils 256 Hosts entstehen.

IPsec

IP Security (IPsec) ist ein Standard, der es ermöglicht, bei IP-Datagrammen (→ Datagramm) die Authentizität des Absenders, die Vertraulichkeit und die Integrität der Daten durch Verschlüsselung zu wahren. Die Bestandteile von IPsec sind der Authentication Header (AH), die Encapsulating-Security-Payload (ESP), die Security Association (SA) und der Internet Key Exchange (IKE).
Zu Beginn der Kommunikation klären die an der Kommunikation beteiligten Rechner das benutzte Verfahren und dessen Implikationen wie z. B. *Transport Mode* oder *Tunnel Mode*
Im *Transport Mode* wird in jedes IP-Datagramm zwischen IP-Header und TCP- bzw. UDP-Header ein IPsec-Header eingesetzt. Da dadurch der IP-Header unverändert bleibt, ist dieser Modus nur für eine Host- zu-Host-Verbindung geeignet.
Im *Tunnel Mode* wird dem gesamten IP-Datagramm ein IPsec-Header und ein neuer IP-Header vorangestellt. D. h. das ursprüngliche Datagramm wird insgesamt verschlüsselt in der Payload des neuen Datagramms untergebracht.
Der *Tunnel Mode* findet beim VPN Anwendung: Die Geräte an den Tunnelenden sorgen für die Ver- bzw. Entschlüsselung der Datagramme, auf der Tunnelstrekke, d. h. auf dem Übertragungsweg über ein öffentliches Netz bleiben die eigentlichen Datagramme vollständig geschützt.

NAT (Network Address Translation)

Bei der Network Address Translation (NAT) - oft auch als *IP-Masquerading* bezeichnet - wird hinter einem einzigen Gerät, dem sog. NAT-Router, ein ganzes Netzwerk „versteckt“. Die internen Rechner im lokalen Netz bleiben mit ihren IP-Adressen verborgen, wenn Sie nach außen über die NAT-Router kommunizieren. Für die Kommunikationspartner außen erscheint nur der NAT-Router mit seiner eigenen IP-Adresse.
Damit interne Rechner dennoch direkt mit externen Rechnern (im Internet) kommunizieren können, muss der NAT-Router die IP-Datagramme verändern, die von internen Rechnern nach außen und von außen zu einem internen Rechner gehen.
Wird ein IP-Datagramm aus dem internen Netz nach außen versendet, verändert der NAT-Router den UDP- bzw. TCP-Header des Datagramms. Er tauscht die Quell-IP-Adresse und den Quell-Port aus gegen die eigene offizielle IP-Adresse und einen eigenen, bisher unbenutzen Port. Dazu führt er eine Tabelle, die die Zuordnung der ursprünglichen mit den neuen Werten herstellt.

Beim Empfang eines Antwort-Datagramms erkennt der NAT-Router anhand des angegebenen Zielports, dass das Datagramm eigentlich für einen internen Rechner bestimmt ist. Mit Hilfe der Tabelle tauscht der NAT-Router die Ziel-IP-Adresse und den Ziel-Port aus und schickt das Datagramm weiter ins interne Netz.

Port-Nummer

Bei den Protokollen UDP und TCP wird jedem Teilnehmer eine Portnummer zugeordnet. Über sie ist es möglich zwischen zwei Rechnern mehrere UDP oder TCP Verbindungen zu unterscheiden und somit gleichzeitig zu nutzen.
Bestimmte Portnummern sind für spezielle Zwecke reserviert. Zum Beispiel werden in der Regel HTTP Verbindungen zu TCP Port 80 oder POP3 Verbindungen zu TCP Port 110 aufgebaut.

Proxy

Ein Proxy (Stellvertreter) ist ein zwischengeschalteter Dienst. Ein Web-Proxy (z. B. Squid) wird gerne vor ein größeres Netzwerk geschaltet. Wenn z. B. 100 Mitarbeiter gehäuft auf eine bestimmte Website zugreifen und dabei über den Web-Proxy gehen, dann lädt der Proxy die entsprechenden Seiten nur einmal vom Server und teilt sie dann nach Bedarf an die anfragenden Mitarbeiter aus. Dadurch wird der Trafic nach außen reduziert, was Kosten spart.

PPPoE

Akronym für **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet. Basiert auf den Standards PPP und Ethernet. PPPoE ist eine Spezifikation, um Benutzer per Ethernet mit dem Internet zu verbinden über ein gemeinsam benutztes Breitbandmedium wie DSL, Wireless LAN oder Kabel-Modem.

PPTP

Akronym für **P**oint-to-**P**oint **T**unneling **P**rotocol. Entwickelt von Microsoft, U.S. Robotics und anderen wurde dieses Protokoll entwickelt, um zwischen zwei VPN-Knoten (→ VPN) über ein öffentliches Netz sicher Daten zu übertragen.

Router

Ein Router ist ein Gerät, das an unterschiedliche IP-Netze angeschlossen ist und zwischen diesen vermittelt. Dazu besitzt er für jedes an ihn angeschlossene Netz eine Schnittstelle (= Interface). Beim Eintreffen von Daten muss ein Router den richtigen Weg zum Ziel und damit die passende Schnittstelle bestimmen, über welche die Daten weiterzuleiten sind. Dazu bedient er sich einer lokal vorhandenen Routingtabelle, die angibt, über welchen Anschluss des Routers (bzw. welche Zwischenstation) welches Netzwerk erreichbar ist.
Dabei werden die durchgeleiteten IP-Pakete so umgeschrieben, als wenn sie vom Router selber kommen und nicht von einem der Rechner des angeschlossenen Netzes. Dieses Verfahren wird NAT (Network Address Translation) genannt. (→ NAT)

Trap

Vor allem in großen Netzwerken findet neben den anderen Protokollen zusätzlich das SNMP Protokoll (Simple Network Management Protocol) Verwendung. Dieses UDP-basierte Protokoll dient zur zentralen Administrierung von Netzwerkgeräten. Zum Beispiel kann man mit dem Befehl GET eine Konfigurationen abfragen, mit dem Befehl SET die Konfiguration eines Gerätes ändern, vorausgesetzt, das so angesprochene Netzwerkgerät ist SNMP-fähig.
Ein SNMP-fähiges Gerät kann zudem von sich aus SNMP-Nachrichten verschikken, z. B. wenn außergewöhnliche Ereignisse auftreten. Solche Nachrichten nennt man SNMP Traps.

X.509 Zertifikat

Eine Art „Siegel“, welches die Echtheit eines öffentlichen Schlüssels (→ asymmetrische Verschlüsselung) und zugehöriger Daten belegt.
Damit der Benutzer eines zum Verschlüsseln dienenden öffentlichen Schlüssels

sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von seinem tatsächlichen Aussteller und damit der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung. Diese Beglaubigung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Ausstellers mit seinem Schlüssel übernimmt eine zertifizierende Stelle (*Certification Authority - CA*). Dies geschieht nach den Regeln der CA, indem der Aussteller des öffentlichen Schlüssels beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Überprüfung signiert die CA den öffentliche Schlüssel mit ihrer (digitalen) Unterschrift, ihrer Signatur. Es entsteht ein Zertifikat.

Ein X.509(v3) Zertifikat beinhaltet also einen öffentlichen Schlüssel, Informationen über den Schlüsseleigentümer (angegeben als Distinguised Name (DN)), erlaubte Verwendungszwecke usw. und die Signatur der CA.

Die Signatur entsteht wie folgt: Aus der Bitfolge des öffentlichen Schlüssels, den Daten über seinen Inhaber und aus weiteren Daten erzeugt die CA eine individuelle Bitfolge, die bis zu 160 Bit lang sein kann, den sog. HASH-Wert. Diesen verschlüsselt die CA mit ihrem privaten Schlüssel und fügt ihn dem Zertifikat hinzu. Durch die Verschlüsselung mit dem privaten Schlüssel der CA ist die Echtheit belegt, d. h. die verschlüsselte HASH-Zeichenfolge ist die digitale Unterschrift der CA, ihre Signatur. Sollten die Daten des Zertifikats missbräuchlich geändert werden, stimmt dieser HASH-Wert nicht mehr, das Zertifikat ist dann wertlos.

Der HASH-Wert wird auch als Fingerabdruck bezeichnet. Da er mit dem privaten Schlüssel der CA verschlüsselt ist, kann jeder, der den zugehörigen öffentlichen Schlüssel besitzt, die Bitfolge entschlüsseln und damit die Echtheit dieses Fingerabdrucks bzw. dieser Unterschrift überprüfen.

Durch die Heranziehung von Beglaubigungsstellen ist es möglich, dass nicht jeder Schlüsseleigentümer den anderen kennen muss, sondern nur die benutzte Beglaubigungsstelle. Die zusätzlichen Informationen zu dem Schlüssel vereinfachen zudem die Administrierbarkeit des Schlüssels.

X.509 Zertifikate kommen z.B. bei Email Verschlüsselung mittels S/MIME oder IPsec zum Einsatz.

Protokoll, Übertragungsprotokoll

Geräte, die miteinander kommunizieren, müssen dieselben Regeln dazu verwenden. Sie müssen dieselbe „Sprache sprechen“. Solche Regeln und Standards bezeichnet man als Protokoll bzw. Übertragungsprotokoll. Oft benutze Protokolle sind z. B. IP, TCP, PPP, HTTP oder SMTP.

Service Provider

Anbieter, Firma, Institution, die Nutzern den Zugang zum Internet oder zu einem Online-Dienst verschafft.

Spoofing, Antispoofing

In der Internet-Terminologie bedeutet Spoofing die Angabe einer falschen Adresse. Durch die falsche Internet-Adresse täuscht jemand vor, ein autorisierter Benutzer zu sein.

Unter Anti-Spoofing versteht man Mechanismen, die Spoofing entdecken oder verhindern.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung werden Daten mit dem gleichen Schlüssel ver- und entschlüsselt. Beispiele für symmetrische Verschlüsselungsalgorithmen sind DES und AES. Sie sind schnell, jedoch bei steigender Nutzerzahl nur aufwendig administrierbar.

TCP/IP (Transmission Control Protocol/ Internet Protocol)

Netzwerkprotokolle, die für die Verbindung zweier Rechner im Internet verwendet werden.
IP ist das Basisprotokoll.
UDP baut auf IP auf und verschickt einzelne Pakete. Diese können beim Empfänger in einer anderen Reihenfolge als der abgeschickten ankommen, oder sie können sogar verloren gehen.
TCP dient zur Sicherung der Verbindung und sorgt beispielsweise dafür, dass die Datenpakete in der richtigen Reihenfolge an die Anwendung weitergegeben werden.
UDP und TCP bringen zusätzlich zu den IP-Adressen Port-Nummern zwischen 1 und 65535 mit, über die die unterschiedlichen Dienste unterschieden werden.
Auf UDP und TCP bauen eine Reihe weiterer Protokolle auf, z. B. HTTP (Hyper Text Transfer Protokoll), HTTPS (Secure Hyper Text Transfer Protokoll), SMTP (Simple Mail Transfer Protokoll), POP3 (Post Office Protokoll, Version 3), DNS (Domain Name Service).
ICMP baut auf IP auf und enthält Kontrollnachrichten.
SMTP ist ein auf TCP basierendes E-Mail-Protokoll.
IKE ist ein auf UDP basierendes IPsec-Protokoll.
ESP ist ein auf IP basierendes IPsec-Protokoll.
Auf einem Windows-PC übernimmt die WINSOCK.DLL (oder WSOCK32.DLL) die Abwicklung der beiden Protokolle.
(→ Datagramm)

VLAN

Über ein VLAN (Virtual Local Area Network) kann man ein physikalisches Netzwerk logisch in getrennte, nebeneinander existierende Netze unterteilen. Die Geräte der unterschiedlichen VLANs können dabei nur Geräte in ihrem eigenen VLAN erreichen. Die Zuordnung zu einem VLAN wird damit nicht mehr nur allein von der Topologie des Netzes bestimmt, sondern auch durch die konfigurierte VLAN ID.

Die VLAN Einstellung kann als optionale Einstellung zu jeder IP vorgenommen werden. Ein VLAN wird dabei durch seine VLAN ID (1-4094) identifiziert. Alle Geräte mit der selben VLAN ID gehören dem gleichen VLAN an und können miteinander kommunizieren.
Das Ethernet-Paket wird für VLAN nach IEEE 802.1Q um 4 Byte erweitert, davon stehen 12 Bit zur Aufnahme der VLAN ID zur Verfügung. Die VLAN ID „0“ und „4095“ sind reserviert und nicht zur Identifikation eines VLANs nutzbar.

VPN (Virtuelles Privates Netzwerk)

Ein **V**irtuelles **P**rivates **N**etzwerk (VPN) schließt mehrere voneinander getrennte private Netzwerke (Teilnetze) über ein öffentliches Netz, z. B. das Internet, zu einem gemeinsamen Netzwerk zusammen. Durch Verwendung kryptographischer Protokolle wird dabei die Vertraulichkeit und Authentizität gewahrt. Ein VPN bietet somit eine kostengünstige Alternative gegenüber Standleitungen, wenn es darum geht, ein überregionales Firmennetz aufzubauen.

9 Technische Daten

Allgemein

CPU	Intel IXP 42x mit 266 MHz (bzw. 533 MHz industrial und enterprise XL)
Speicher	16 MB Flash, 64 MB SDRAM
LAN u. WAN Schnittstellen	Ethernet IEEE 802 10/100 Mbps RJ45
Seriell	RS 232
Stromversorgung	smart: Via USB-Schnittstelle (5 V, 500 mA) oder durch externes Netzteil (110 - 230 V) delta: 5VDC, 3A
Betriebssystem	Innominate Embedded Linux
Funktionsüberwachung	Watchdog und optische Anzeige
Relative Luftfeuchtigkeit	blade, smart, PCI: max. 90 % (nicht kondensierend) delta: 5-95% (nicht kondensierend)
Umgebungstemperatur	smart, blade: 0-40°C industrial: bis 70°C delta: -20°C bis 70°C PCI: 0-55°C

mGuard industrial

Netzausdehnung	Länge eines 10BASE-T/100BASE-TX Twisted Pair-Segmentes ca. 100 m
Betriebsspannung	NEC Class 2 power source 12VDC bzw. 24VDC -25% +33% Sicherheitskleinspannung (SELV/PELV, redundante Eingänge entkoppelt), max. 5A. Pufferzeit: min. 10 ms bei 24VDC
Potentialdifferenz zwischen Eingangsspannung und Gehäuse	Potentialdifferenz zu Eingangsspannung +24 VDC: 32 VDC Potentialdifferenz zu Eingangsspannung Masse: -32 VDC
Leistungsaufnahme	max. 7,2 W bei 24 VDC; 24,6 Btu (IT)/h
Überstromschutz am Eingang	nicht wechselbare Schmelzsicherung
Abmessungen	B x H x T 46 mm x 131 mm x 111 mm
Masse	340 g
Umgebungstemperatur	Umgebende Luft 0 ºC bis + 60 ºC
Lagerungstemperatur	Umgebende Luft - 40 ºC bis + 70 ºC
Relative Luftfeuchtigkeit	10% bis 95% (nicht kondensierend)

Luftdruck	geignet bis 2000 m (795 hPa)
Verschmutzungsgrad	2
EMV-Störfestigkeit	Entladung statischer Elektrizität Kontaktentladung: EN 61000-4-2 Prüfschärfegrad 3 Luftentladung: EN 61000-4-2 Prüfschärfegrad 3 Elektromagnetische Felder: EN 61000-4-3 Prüfschärfegrad 3 Schnelle Transienten: EN 61000-4-4 Prüfschärfegrad 3 Stoßspannungen symmetrisch: EN 61000-4-5 Prüfschärfegrad 2 Stoßspannungen unsymmetrisch: EN 61000-4-5 Prüfschärfegrad 3 Leitungsgebundene HF-Störungen: EN 61000-4-6 Prüfschärfegrad 3
EMV-Störaussendung	EN 55022: Class A FCC 47 CFR Part 15: Class A Germanischer Lloyd: Klassifizierungs- und Bauvorschriften VI-7-3 Teil1 Ed.2003
Festigkeit	Vibration EC 60068-2-6 Test FC Prüfschärfegrade nach IEC 61131-2 E2 CDV und Germanischer Lloyd Richtlinien für die Durchführung von Baumusterprüfungen Teil 1 Schock EC 60068-2-27 Test Ea Prüfschärfegrad nach IEC 61131-2 E2 CDV
Zertifizierungen	cUL 508 / CSA 22.2 No.142 erfüllt cUL 1604 / CSA 22.2 No.213 angemeldet Germanischer Lloyd erfüllt

Notes on CE identification

This device comply with the regulations of the following European directive: 89/336/EEC Council Directive on the harmonization of the legal regulations of member states on electromagnetic compatibility (amended by Directives 91/263/EEC, 92/31/EEC and 93/68/EEC).

The EU declaration of conformity is kept available for the responsible authorities in accordance with the above-mentioned EU directives at:

Innominate Security Technologies AG
Albert-Einstein-Str. 14
D-12489 Berlin
Telephone ++49 (0)30 6392-3300

The product can be used in the residential sphere (residential sphere, business and trade sphere and small companies) and in the industrial sphere.

- Interference proof:
  EN 61000-6-2:2001
- Emitted immunity:
  EN 55022:1998

+ A1 2000
+ A2 2003, Class A

FCC Note

This equipment has been tested and found to comply with the limits for a Class A digital device, persuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.